CDP Private Cloud Data Services 1.5.4

CDP Private Cloud Data Services Release Notes

Date published: 2023-12-16
Date modified: 2024-07-31

https://docs.cloudera.com/

Legal Notice

Contents

What's new in CDP Private Cloud Data Services 1.5.4

New features in the 1.5.4 release of the CDP Private Cloud Management Console service.

CDP Private Cloud Data Services 1.5.4 support with 7.1.9 SP1.

Note: Cloudera Manager 7.11.3 CHF7 Data Services (version: 7.11.3.14) support CDP Private Cloud Data Services 1.5.4 release.

Note: Cloudera Manager 7.11.3 CHF8 does not support any CDP Private Cloud Data Services release.

Certifications

- Base (7.1.9 CHF 6, 7.1.7 SP3, 7.1.8 CHF22)
- CM 7.11.3 CHF 6 and CHF7
- Iceberg v2 GA on CDW, CDE, & CML with Ozone
- OEL (RHCK Kernel Only) 8.7, 8.8, 8.9, 9.1, 9.2, 9.3
- RHEL 8.7, 8.8, 8.9, 9.1, 9.2, 9.3
- K8s 1.27 and OCP 4.14

Stability and Resiliency: New prerequisite check in ECS Install Wizard

A new step is added in the ECS Install Wizard called Check Prerequisites. This ECS prerequisite checks fresh installations seamlessly and improves the overall installation experience for administrators. This step checks if the ECS hosts meet a list of minimum requirements before installation. For more information on this prerequisite check, see Installing CDP Private Cloud Data Services using ECS.

DRS automatic backups

Starting from CDP Private Cloud Data Services 1.5.4, DRS automatic backups for Control Plane, Cloudera Data Warehouse (CDW), and Cloudera Data Engineering (CDE) are enabled by default on ECS clusters for new installations or after cluster upgrade to version 1.5.4 or higher. You can disable this option, if required. You can also configure the external storage in Longhorn for ECS, and then initiate DRS automatic backups to it.

Automatic backups (DRS) functionality is disabled by default on OCP clusters.

For more information, see DRS automatic backups.

Authentication for Ingress TLS/SSL

A new property (ssl_private_key_password) is added to the Cloudera Manager to specify the password for the private key in the Ingress Controller TLS/SSL Server Certificate and Private Key file.

Improved Diagnostics

The tez-site.xml file is now included in the Management Console diagnostic bundle download.

Known issues for the CDP Private Cloud Data Services 1.5.4

This section lists known issues that you might run into while using the CDP Private Cloud Management Console service.

Known Issues in Management Console 1.5.4

OPSX-5147: OOM when retrieving size of Binary File

Sometimes, diagnostics bundle collection fails to complete due to OOM issues.

Limit the time range for the diagnostics bundle.

OPSX-5148: Diagnostics Collection from UI w/ Default No Time Limit Should Not Invoke Timestamp Filtering

When the diagnostics collection is triggered through the UI, by default, "No Time Limit" is selected. Filtering of logs by timestamp is still observed.

No workaround available.

DOCS-20088/OPSX-4781: Vault pods may take long time to be ready during upgrades from 1.5.2 to 1.5.3

The 'vault-0' pod takes longer time to attach volume in some upgrade cases than usual. Due to the excess time taken the cluster upgrade may fail. But, usually in 15 minutes the volume can attach automatically and the pod would start running. In that case, the user can resume the upgrade.

No workaround available.

OPSX-5155: OS Upgrade | Pods are not starting after the OS upgrade from RHEL 8.6 to 8.8

After an OS upgrade and start of the ECS service, pods fail to come up due to stale state.

Restart the ECS cluster.

OPSX-5055: ECS upgrade failed at Unseal Vault step

During an ECS upgrade from 1.5.2 to 1.5.4 release, the vault pod fails to start due to an error caused by the Longhorn volume unable to attach to the host. The error is as below:

Warning FailedAttachVolume 3m16s (x166 over 5h26m) attachdetach-controller AttachVolume.Attach failed for volume "pvc-0ba86385-9064-4ef9-9019-71976b4902a5" : rpc error: code = Internal desc = volume pvc-0ba86385-9064-4ef9-9019-71976b4902a5 failed to attach to node host-1.cloudera.com with attachmentID csi-7659ab0e6655d308d2316536269de47b4e66062539f135bf6012bfc8b41fc345: the volume is currently attached to different node host-2.cloudera.com

Follow below steps provided by SUSE to ensure the Longhorn volume is correctly attached to the node where the vault pod is running.

```
# Find out the volume name that is failing to attach to the vault
 pod.
For e.g. pvc-bc73e7d3-c7e7-468a-b8e0-afdb8033e40b from the pod
logs.
kubectl edit volumeattachments.longhorn.io -n longhorn-system
pvc-bc73e7d3-c7e7-468a-b8e0-afdb8033e40b

# Update the "spec:" section of the volumeattachment and replace
attachmentTickets section with {} as shown below and save.
spec:
 attachmentTickets: {}
 volume: pvc-bc73e7d3-c7e7-468a-b8e0-afdb8033e40b

# scale down the vault statefulset to 0 and scale it back up.
kubectl scale sts vault --replicas=0 -n vault-system
kubectl scale sts vault --replicas=1 -n vault-system
```

OPSX-4308: Display error in UI if listEnvironments failed

On the Environments page, if the `listEnvironments` API call fails, the error is hidden, and instead no environments are displayed, even though they do exist. This can be due to vault issues or connectivity issues.

No workaround available but the register environment page shows the error.

OPSX-4684: Start ECS command shows green(finished) even though start docker server failed on one of the hosts

The Docker service starts, but one or more Docker roles fail to start because the corresponding host is unhealthy.

Ensure the host is healthy. Start the the Docker role on the host.

OPSX-735: Kerberos service should handle Cloudera Manager downtime

The Cloudera Manager Server in the base cluster operates to generate Kerberos principals for Private Cloud. If there is downtime, you may observe Kerberos-related errors.

Resolve downtime on Cloudera Manager. If you encounter Kerberos errors, you can retry the operation (such as retrying creation of the Virtual Warehouse).

Known Issues in Management Console 1.5.3

OPSX-4754 [ECS Restart Stability] DaemonSet rollout process is stuck post rolling restart where DaemonSet kube-system/rke2-canal has not finished or progressed for at least 15 minutes

On RHEL 9.x, an ECS service DaemonSet rollout health alert appears in the Cloudera Manager after an ECS installation and a rolling restart.

To fix the DaemonSet rollout issue:

1. Edit the DaemonSet rke2-canal configuration file by running the following command:

```
KUBECTL -n kube-system edit ds/rke2-canal
```

   Change the value of felixIptablesBackend from auto to Legacy and save the DaemonSet rke2-canal configuration file.
2. Reboot each node one-by-one.
3. Check to see if any of the nodes are cordoned off. If so, uncordon them:

```
[root@host-1 ~]# $KUBECTL get nodes
                  NAME STATUS ROLES AGE VERSION
                  host-1.ecs-restart1.kcloud.cloudera.com Re
ady,SchedulingDisabled control-plane,etcd,master 17h v1.26.1
0+rke2r1
                  host-2.ecs-restart1.kcloud.cloudera.com R
eady <none> 17h v1.26.10+rke2r1
                  host-3.ecs-restart1.kcloud.cloudera.com Re
ady <none> 17h v1.26.10+rke2r1
                  host-4.ecs-restart1.kcloud.cloudera.com Rea
dy <none> 17h v1.26.10+rke2r1
                  [root@host-1 ~]# $KUBECTL uncordon host-1.ec
s-restart1.kcloud.cloudera.com
                  node/host-1.ecs-restart1.kcloud.cloudera.com
 uncordoned
                  [root@host-1 ~]# $KUBECTL get nodes
                  NAME STATUS ROLES AGE VERSION
                  host-1.ecs-restart1.kcloud.cloudera.com Rea
dy control-plane,etcd,master 17h v1.26.10+rke2r1
                  host-2.ecs-restart1.kcloud.cloudera.com R
eady <none> 17h v1.26.10+rke2r1
                  host-3.ecs-restart1.kcloud.cloudera.com Re
ady <none> 17h v1.26.10+rke2r1
                  host-4.ecs-restart1.kcloud.cloudera.com Rea
dy <none> 17h v1.26.10+rke2r1
                  [root@host-1 ~]#
```

4. Ensure that the Vault is unsealed. , To unseal the vault in Cloudera Manager navigate to Clusters ECS <***ECS SERVICES***> such as ECS-1 or ECS-2 Actions Unseal Vault .
5. Wait for five to six minutes.
6. Check for longhorn pods that fail to come up on any of the hosts:

```
[root@host-1 ~]# kubectl -o wide get pods -n longhorn-system |
 grep -v "Running" | grep -v "Completed"
NAMESPACE                                NAME
                                             READY
STATUS                  RESTARTS         AGE     IP
  NODE
NOMINATED NODE   READINESS GATES
longhorn-system                          longhorn-csi-plugin-
frwnw                                         2/3
CrashLoopBackOff        14 (3m51s ago)   6h20m   10.x.x.x
 host-1.upgr-ecs-ext.kcloud.cloudera.com    <none>
          <none>
longhorn-system                          longhorn-manager-lgzm
b                                             0/1
CrashLoopBackOff        7 (97s ago)      6h24m   10.x.x.x
host-1.upgr-ecs-ext.kcloud.cloudera.com    <none>
          <none>
```

7. Reboot the host (In this case the host is: *host-1.upgr-ecs-ext.kcloud.cloudera.com*).
8. Wait for 15-30 minutes for pods to come up.
9. Post ECS reboot, if you notice buildkit pods in the following CrashLoopBackOff state, then delete those buildkit pods:

```
[root@host-1 ~]# kubectl -o wide get pods | grep -v "Running"
 | grep -v "Completed"
NAMESPACE                                NAME
                                             READY   STATUS
               RESTARTS         AGE     IP             NODE
                                    NOMINATED NODE   READINESS
 GATES
quasar-skl2-host-1                           buildkit-2jdmw
                                       2/3     CrashLoopBackOff
        14 (3m51s ago)   6h20m   10.x.x.x     host-1.upgr-ecs-
ext.kcloud.cloudera.com    <none>           <none>
quasar-skl2-host-1                         buildkit-k20smc
                                           0/1     CrashLoopBa
ckOff        7 (97s ago)      6h24m   10.x.x.x     host-2.up
gr-ecs-ext.kcloud.cloudera.com    <none>           <none>
```

You can delete the above buildkit pods by one of the following ways:

- On the Cloudera Manager UI, navigate to Clusters ECS <***ECS SERVICES***> such as ECS-1 or ECS-2 Web UI ECS Web UI Delete .
- Run the following command to delete all such buildkit pods:

```
[root@host-1 ~]# kubectl delete pod buildkit-2jdmw -n quasar
-skl2-host-1
```

Wait for the buildkit pods to start back up.

OPSAPS-69892: kube-proxy failure causing issues with cluster

After rebooting/restarting an ECS agent node, the kube-proxy Linux process may not start due to a race condition in the kubelet. When this happens, ECS cluster networking and other services – such as Vault, DNS, authentication, Longhorn storage, etc. – are affected. At the Kubernetes pod level, errors such as "connection refused", "connection timed out" and "i/o timeout" may be observed. If

you suspect possible networking issues in your ECS cluster, checking kube-proxy is a good first step.

To fix this issue, perform the following steps on all of the affected nodes:

1. To identify which agent needs to be restarted, check the status of each kube-proxy pod to make sure it is in the "ready" state by running the following command on each host in the cluster.

   ```
   kubectl describe pod [***POD-NAME***] -n kube-system
   ```

   Here, *[***POD-NAME***]* should have a format such as: kube-proxy-<hostname>.

   In the Conditions section of the describe pod output, confirm that the "ready" condition is "True".

   ```
   Conditions:
     Type              Status
     Initialized       True
     Ready             True
     ContainersReady   True
     PodScheduled      True
   ```

   Another option is to run the following command:

   ```
   kubectl get pods -n kube-system -l component=kube-proxy -o go-
   template='{{range .items}}
   {{.metadata.name}}{{"\n"}}{{"  "}}{{range .status.conditions}}
   {{ if eq .type "Ready" }}
   Ready:{{.status}}{{"\n\n"}}{{end}}{{end}}{{end}}'
   ```

   The sample output displays the status of all of the kube-proxy pods in the cluster:

   ```
   kube-proxy-host-1.cloudera.com
     Ready:True

   kube-proxy-host-2.cloudera.com
     Ready:True

   kube-proxy-host-3.cloudera.com
     Ready:True
   ```

2. If the "ready" state is False, kube-proxy is not functioning properly, regardless of whether the kube-proxy process is running on that host or not. On each of the affected nodes, run the following command to delete the kube-proxy pod manifest:

   ```
   rm /var/lib/rancher/rke2/agent/pod-manifests/kube-proxy.yaml
   ```

3. Start the agent role.

   After the agent role is started, you may not immediately see the kube-proxy process running, but a new kube-proxy process should start shortly. Check the pod status to make sure it is ready. After all of the problem agents have been restarted, the cluster may complain that the vault is sealed – if so, unseal it. At this point, the Control Plane should be functioning properly.

Additional details about this issue are available here: https://www.suse.com/support/kb/doc/?id=000021284

OPSX-4766: [ECS Restart]| Host Reboot | start command failed with error - "Timed out waiting for kube-apiserver to be ready"

In an ECS cluster with HA enabled, ECS Start fails with an error after stopping the cluster and rebooting the hosts.

Steps to reproduce:

1. Stop ECS.
2. Reboot hosts.
3. Start ECS.

The start command fails with the following error message:

"Timed out waiting for kube-apiserver to be ready"

Option 1:

Start each master role instance individually without waiting each node to be up and running.

Option 2:

If Option 1 does not work, follow the steps from SUSE to recover the cluster:https://docs.rke2.io/backup_restore#cluster-reset

Known Issues in Management Console 1.5.2

OPSAPS-68923: CM - After CM upgrade from 7.9.5 to 7.11.3.x ECS cluster showing stale config

After Cloudera Manager upgrade from 7.9.5 to 7.11.3.x, an ECS 1.5.0 cluster may show a stale config to add ""limit_fds": 1048576"

This can be ignored – no restart of the ECS cluster is necessary. When the ECS 1.5.0 cluster is upgraded to 1.5.2, the stale config will be resolved.

OPSX-4594: [ECS Restart Stability] Post rolling restart few volumes are in detached state (vault being one of them)

After rolling restart there may be some volumes in detached state.

1. Open the Longhorn UI to view the detached volumes.
2. Perform the following operations for each volume in a detached state:
   a. Identify the workload name and type from the volume details.
   b. Identify the workload and number of replicas using kubectl or the Kubernetes UI.
   c. Scale the workload down to 0.
   d. Wait for the pods associated with the workload to fully terminate.
   e. Scale up the workload up to the number of replicas it had originally.

To prevent this issue, use the Longhorn UI to set the number of replicas for the volume to at least 3.

OPSAPS-68558: [7.9.5->7.11.3.2] CM upgrade failed with BeanCreationException: Error creating bean with name 'com.cloudera.server.cmf.TrialState'

After upgrading the Cloudera Manager package, the Cloudera Manager Server does not start. An error about "Active Commands" is shown in the Cloudera Manager Server log.

This may happen when the Private Cloud Data Services Control Plane is actively issuing requests to Cloudera Manager while an upgrade is being performed.

Before upgrading Cloudera Manager make sure there are no active commands. If there are any active commands, wait for them to complete before starting a Cloudera Manager upgrade.

If Cloudera Manager restart fails after upgrade due to an active getClientConfig command, check the Cloudera Manager server log for a "There are 1 active commands of type GetClientConfigFiles" error. This may block a Cloudera Manager restart after upgrade. Use the following steps to resolve this issue:

1. Login to Cloudera Manager database.

2. Search for any active GetClientConfigFiles command in the COMMANDS table.

```
UPDATE COMMANDS SET active=0,success=false,state='CANCELLED'
 where command_id=<command_id>;
```

3. Delete these entries, including foreign key dependencies, in the following tables:
   - PROCESSES
   - PROCESSES_DETAIL
   - COMMANDS_DETAIL

```
cm=> DELETE FROM COMMANDS where command_id=1546340765;
ERROR:  update or delete on table "commands" violates foreign
 key constraint "fk_process_command" on table "processes"
DETAIL:  Key (command_id)=(1546340765) is still referenced fro
m table "processes".
cm=>
cm=> DELETE FROM processes where command_id=1546340765;
ERROR:  update or delete on table "processes" violates foreign
 key constraint "fk_processes_detail_process" on table "proc
esses_detail"
DETAIL:  Key (process_id)=(1546340766) is still referenced fro
m table "processes_detail".
cm=>
cm=>                                          ^
cm=> DELETE FROM processes_detail where process_id=1546340766;
DELETE 1
cm=> DELETE FROM processes where command_id=1546340765;
DELETE 1
cm=> DELETE FROM COMMANDS where command_id=1546340765;
ERROR:  update or delete on table "commands" violates foreign
 key constraint "fk_commands_detail_command" on table "comma
nds_detail"
DETAIL:  Key (command_id)=(1546340765) is still referenced f
rom table "commands_detail".
cm=>
cm=> DELETE FROM commands_detail where command_id=1546340765;
DELETE 1
cm=> DELETE FROM COMMANDS where command_id=1546340765;
DELETE 1
```

4. Restart the Cloudera Manager server.

OPSX-4392: Getting the real client IP address in the application

CML has a feature for adding the audit event for each user action (Monitoring User Events). In Private Cloud, instead of the client IP, we are getting the internal IP, which is logged into the internal DB.

In ECS, add the enable-real-ip configuration as true for the nginx ingress controller:

```
apiVersion: v1
data:
  allow-snippet-annotations: "true"
  enable-real-ip: "true"                    <<<<<<<<<< new config
kind: ConfigMap
metadata:
  annotations:
    meta.helm.sh/release-name: rke2-ingress-nginx
    meta.helm.sh/release-namespace: kube-system
  creationTimestamp: "2023-05-09T04:54:53Z"
  labels:
    app.kubernetes.io/component: controller
    app.kubernetes.io/instance: rke2-ingress-nginx
```

```
    app.kubernetes.io/managed-by: Helm
    app.kubernetes.io/name: rke2-ingress-nginx
    app.kubernetes.io/part-of: rke2-ingress-nginx
    app.kubernetes.io/version: 1.6.4
    helm.sh/chart: rke2-ingress-nginx-4.5.201
  name: rke2-ingress-nginx-controller
  namespace: kube-system
  resourceVersion: "162559439"
  uid: cca67b0c-bc05-4e1f-8439-7d44323f4624
```

In OCP, you may be able configure this using HAproxy with X-forward-for pass to OpenShift 4.

OPSX-4552: [ECS Restart] One of the docker servers failed to come up after starting the cluster post hosts reboot

At times the Docker server may fail to come up and return the following error message:

/var/run/docker.sock: Is a directory

On the Docker server role host, remove the /var/run/docker.sock directory, then restart the Docker server role.

CDPVC-1137, CDPAM-4388, COMPX-15083, and COMPX-15418: OpenShift Container Platform version upgrade from 4.10 to 4.11 fails due to a Pod Disruption Budget (PDB) issue

PDB can prevent a node from draining which makes the nodes to report the "Ready,SchedulingDisabled" state. As a result, the node is not updated to correct the Kubernetes version when you upgrade OCP from 4.10 to 4.11.

To resolve this issue, confirm that the upgrade has failed due to the PDB issue, and then manually delete the PDBs from the Private Cloud namespace.

1. Run the following command to check whether the nodes are stuck in the "Ready,SchedulingDisabled" state:

   ```
   oc get nodes
   ```

2. Get the machine config daemon details of the particular pod as follows:

   ```
   oc get po -n openshift-machine-config-operator -l 'k8s-app=m
   achine-config-daemon' -o wide
   ```

3. Check the logs of the machine config operator of that particular node as follows:

```
oc logs -f -n openshift-machine-config-operator [***MACHINE-CONFIG-DAEMON-NAME***] -c machine-config-daemon
```

Replace *[***MACHINE-CONFIG-DAEMON-NAME***]* with the actual machine config daemon name.

You may see one of the following errors in the node logs:

- error when evicting pods/cdp-release-cpx-liftie-****" -n "*[***PRIVATE-CLOUD-NAMESPACE***]* Cannot evict pod as it would violate the pod's disruption budget
- error when evicting pods/"cdp-release-cluster-proxy-[******]" -n "*[***PRIVATE-CLOUD-NAMESPACE***]* Cannot evict pod as it would violate the pod's disruption budget

Delete the PDB from the Private Cloud namespace as follows:

a. Obtain the PDB for the cdp-release-cluster-proxy namespace:

```
oc get pdb -n [***PRIVATE-CLOUD-NAMESPACE***] | grep cdp-release-cluster-proxy
```

b. Back up the PDB:

```
oc get pdb [***PDB-NAME-OF-CLUSTER-PROXY***] -n [***PRIVATE-CLOUD-NAMESPACE***] -o yaml >> [***BACKUP-FILE-NAME***].yaml
```

c. Delete the PDB:

```
oc delete pdb [***PDB-NAME-OF-CLUSTER-PROXY***] -n [***PRIVATE-CLOUD-NAMESPACE***]
```

Repeat the steps to delete the cdp-release-cpx-liftie PDB as well.

PULSE-944 and PULSE-941 Observability namespace not created after platform upgrade from 151 to 152

The Cloudera Observability namespace is not created after a platform upgrade from PvC DS 1.5.1 to PvC DS 1.5.2.

During the creation of the resource pool the Cloudera Observability namespace is provided by the CDP Private Cloud Service. If the provisioning flow is not completed, such as due to a timing difference between the start of the computeAPI pod and the call to the computeAPI pod by the service, the namespace is not created.

Trigger the Cloudera Observability namespace deployment by restarting the pvcservice pod.

PULSE-921 Observability namespace has no pods

The Cloudera Observability namespace should have the same number of pods and nodes. When the Cloudera Observability namespace has no pods the prometheus-node-exporter-1.6.0 helm release state becomes invalid and the CDP Private Cloud Service is unable to uninstall and reinstall the namespace. Also, as the Node Exporter is not installed into the Cloudera Observability namespace its metrics are unavailable when querying Prometheus in the control plane, for example the `node_cpu_seconds_total` metric.

Manually uninstall the invalid helm release with the `--debug` flag, verify that there are no helm releases listed by running `-n observability -a`, and then trigger the deployment process by restarting the pvcservice pod in the control plane.

PULSE-697 Add node-exporter to PvC DS

When expanding a cluster with new nodes and there is insufficient CPU and memory resources, the Node Exporter will encounter difficulties deploying new pods on the additional nodes.

To ensure sufficient resource allocation, such as when the Cloudera Observability namespace requires adjustment, delete the existing namespace and restart the pvcservice pod. This automatically initiates the creation of the Cloudera Observability namespace with the appropriate resource allocation.

Note: During the namespace recreation process the Node Exporter metrics are temporarily unavailable.

PULSE-935 Longhorn volumes are over 90% of the capacity alerts on Prometheus volumes

Cloudera Manager displays the following alert about your Prometheus volumes: Concerning: Firing alerts for Longhorn: The actual used space of Longhorn volume is over 90% of the capacity.

Longhorn stores historical data as snapshots that are calculated with the active data for the volume's actual size. This size is therefore greater than the volume's nominal data value.

When the alert is displayed on the Cloudera Manager UI and it is related to Longhorn volumes used by Prometheus, ignore. For more information, see the Longhorn space consumption guidelines in the Longhorn documentation.

PULSE-937 Private-Key field change in Update Remote Write request does not reflect in enabling the metric flow

When using the Management Console UI for Remote Storage the Disable option does not deactivate the remote write configuration, even when the action returns a positive result message. Therefore, when disabling a remote storage configuration use the CLI client to disable the remote storage configuration directly from the API.

At this time when a remote storage configuration is incorrect, do not use the Edit or Disable option from the configuration’s Actions menu (ellipsis icon) to change its configuration. Instead, delete the remote storage's configuration from the configuration’s Actions menu with the Remove Configuration action and then re-create the remote write configuration with the Delete and Create operations of the API, using the CLI client.

PULSE-841 Disabling the remote write configuration logs an error in both cp prometheus and env prometheus

When a metric replication is set up between the cluster and Cloudera Observability and the connection is disabled or deleted, Prometheus writes an error message that states that it cannot replicate the metrics.

No workaround is required. After a few minutes the errors are no longer logged and Prometheus no longer tries to replicate the metrics.

PULSE-895 Disabling the remote write config in the UI is broken in cdp-pvc

The Remote Write Enable and Disable options in the Management Console’s User Interface do not work when a Remote Storage configuration is created with a requestSignerAuth type from either the HTTP API or using the CDP-CLI tool.

At this time, do not use the Enable or Disable options from the Remote Storage configuration’s Actions menu in the Management Console’s UI. Instead, enable or disable the configuration from the HTTP API or using the CDP-CLI tool.

PULSE-936 No Alert to prompt the metric flow being affected b/c of wrong private key configuration

A remote write alert was not triggered when the wrong private key was used in a Remote Storage configuration.

No workaround. Incorrect configuration settings, such as in this case where a bad private key was used, may block the forwarding of metrics. When creating a Remote Storage configuration you must carefully verify each configuration setting.

Known Issues in Management Console 1.5.1

External metadata databases are no longer supported on OCP

As of CDP Private Cloud Data Services 1.5.1, external Control Plane metadata databases are no longer supported. New installs require the use of an embedded Control Plane database. Upgrades from CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1 are supported, but there is currently no migration path from a previous external Control Plane database to the embedded Control Plane database. Upgrades from 1.4.0 or 1.5.0 with external Control Plane metadata databases also require additional steps, which are described in the CDP Private Cloud Data Services 1.5.1 upgrade topics.

DOCS-15855: Networking API is deprecated after upgrade to CDP Private Cloud Data Services 1.5.1 (K8s 1.24)

When the control plane is upgraded from 1.4.1 to 1.5.1, the Kubernates version changes to 1.24. The Livy pods running in existing Virtual Clusters (VCs) use a deprecated networking API for creating ingress for Spark driver pods. Because the old networking API is deprecated and does not exist in Kubernates 1.24, any new job run will not work for the existing VCs.

CDPQE-24295: Update docker client on docker.lab.eng.hortonworks machine

When you attempt to execute the Docker command to fetch the Cloudera-provided images into your air-gapped environment, you may encounter an issue where Docker pulls an incorrect version of the HAProxy image, especially if you are using an outdated Docker client. This situation arises due to the Cloudera registry containing images with multiple platform versions. Unfortunately, older Docker clients may lack the capability to retrieve the appropriate architecture version, such as amd64.

Update the Docker client. It has been demonstrated that Docker 20.10.5 and later versions have been successful in resolving this problem.

OPSX-4266: ECS upgrade from 1.5.0 to 1.5.1 is failing in Cadence schema update job

When upgrading from ECS 1.5.0 to 1.5.1, the CONTROL_PLANE_CANARY fails with the following error:

```
Firing alerts for Control Plane: Job did not complete in time, J
ob failed to complete.
```

And the cdp-release-cdp-cadence-schema-update job fails.

Use the following steps to manually execute the job:

1. Export the job manifest into a file:

```
kubectl get job cdp-release-cdp-cadence-schema-update -n <cdp>
 -o yaml > job.yaml
```

2. Delete the cdp-release-cdp-cadence-schema-update job:

```
kubectl delete job cdp-release-cdp-cadence-schema-update -n
<cdp>
```

3. Remove runtime information from the manifest, such as:

```
resourceVersion
uid
selector
  matchLabels
    controller-uid
labels
  controller-uid
status section
```

4. Create the job:

```
kubectl apply -f job.yaml
```

OPSX-4076:

When you delete an environment after the backup event, the restore operation for the backup does not bring up the environment.

Create the environment manually.

OPSX-4024: CM truststore import into unified truststore should handle duplicate CommonNames

If multiple CA certificates with the exact same value for the Common Name field are present in the Cloudera Manager truststore when a Private Cloud Data Services cluster is installed, only one of them may be imported into the Data Services truststore. This may cause certificate errors if an incorrect/old certificate is imported.

Remove old certificates from the Cloudera Manager truststore, and ensure certificates have unique Common Names.

COMOPS-2822: OCP error x509: certificate signed by unknown authority

The error x509: certificate signed by unknown authority usually means that the Docker daemon that is used by Kubernetes on the managed cluster does not trust the self-signed certificate.

Usually the fix is to copy the certificate to the path below on all of the worker nodes in the cluster:

```
/etc/docker/certs.d/<your_registry_host_name>:<your_registry_hos
t_port>/ca.crt
```

OPSX-3073 [ECS] First run command failed at setup storage step with error "Timed out waiting for local path storage to come up"

Pod stuck in pending state on host for a long time. Error in Role log related to CNI plugin:

Events:

```
   Type     Reason                  Age                    From
  Message
  ----     ------                  ----                   ----
 -------
  Warning  FailedCreatePodSandBox  3m5s (x269 over 61m)  kubelet
 (combined from similar events):
Failed to create pod sandbox: rpc error: code = Unknown desc = f
ailed to setup network for sandbox
"70427e9b26fb014750dfe4441fdfae96cb4d73e3256ff5673217602d503e806
f":
failed to find plugin "calico" in path [/opt/cni/bin]
```

Delete the cni directory on the host failing to launch pods:

ssh root@ecs-ha1-p-7.vpc.cloudera.com rm -rf /var/lib/cni

Restart the canal pod running on that host:

```
kubectl get pods -n kube-system -o wide | grep  ecs-ha1-p-7.vpc.
cloudera.com
kube-proxy-ecs-ha1-p-7.vpc.cloudera.com                1/1
 Running     0          11h   10.65.52.51    ecs-ha1-p-7.vpc.clo
udera.com   <none>           <none>
rke2-canal-llkc9                                       2/2
Running     0          11h   10.65.52.51    ecs-ha1-p-7.vpc.clou
dera.com   <none>           <none>
rke2-ingress-nginx-controller-dqtz8                    1/1     R
unning     0          11h   10.65.52.51    ecs-ha1-p-7.vpc.cloud
era.com   <none>           <none>
kubectl delete pod rke2-canal-llkc9 -n kube-system
```

OPSX-3528: [Pulse] Prometheus config reload fails if multiple remote storage configurations exist with the same name

It is possible to create multiple remote storage configurations with the same name. However, if such a situation occurs, the metrics will not flow to the remote storage as the config reload of the original prometheus will fail.

At any point in time, there should never be multiple remote storage configurations existing that have the same name.

OPSX-1405: Able to create multiple CDP PVC Environments with the same name

If two users try to create an environment with the same name at the same time, it might result in an unusable environment.

Delete the environment and try again with only one user trying to create the environment.

OPSX-1412: Creating a new environment through the CDP CLI reports intermittently that "Environment name is not unique" even though it is unique

When multiple users try to create the same environment at the same time or use automation to create an environment with retries, create environment may fail on collision with a previous request to create an environment.

Delete the existing environment, wait 5 minutes, and try again.

Known Issues in Management Console 1.5.0

Somehow the Rebuilding field inside volume.meta is set to true causing the volume to get stuck in attaching/detaching loop

This is a condition that can occur in ECS Longhorn storage.

Since the volume has only 1 replica in this case, we can:

1. Scale down the workload. The Longhorn volume will be detached.

2. Wait for the Longhorn volume to be detached.

3. SSH into the node that has the replica.

4. cd into the replica folder (for example, /longhorn/replicas/pvc-126d40e2-7bff-4679-a310-e444e84df267-1a5dc941).

5. Change the"Rebuilding" field from true to false in the volume.meta file.

6. Scale up the workload to attach the volume.

Known Issues in Management Console identified before 1.5.0

INSIGHT-2469: COE Insight from case 922848: Not able to connect to bit bucket

After installing CML on an ECS cluster, users were not able to connect the internal bitbucket repo.

Workaround:

In this case the MTU of the ECS virtual network interfaces were larger than that of host external interface, which may cause the network requests from ECS containers to get truncated.

The Container Network Interface (CNI) is a framework for dynamically configuring networking resources. CNI integrates smoothly with Kubenetes to enable the use of an overlay or underlay network to automatically configure the network between pods. Cloudera ECS uses Calico as the CNI network provider.

The MTU of the pods' virtual network interface can be seen by running the ifconfig command.

The default MTU of the virtual network interfaces is 1450.

The MTU setting of the virtual interfaces is stored as a configmap in the kube-system namespace. To modify the MTU, edit the rke2-canal-config configmap.

```
$ /var/lib/rancher/rke2/bin/kubectl --kubeconfig
 /etc/rancher/rke2/rke2.yaml --namespace kube-system
 edit cm rke2-canal-config
```

Find the veth_mtu parameter in the YAML content. Modify the default value of 1450 to the required MTU size.

Next, restart the rke2-canal pods from the kube-system namespace. There will be rke2-canal pods for each ECS node.

After the pods are restarted, all subsequent new pods will use the new MTU setting. However, existing pods that are already running will remain on the old MTU setting. Restart all of the pods to apply the new MTU setting.

OPSX-2484: FileAlreadyExistsException during timestamp filtering

The timestamp filtering may result in FileAlreadyExistsException when there is a file with same name already existing in the tmp directory.

None

OPSX-2772: For Account Administrator user, update roles functionality should be disabled

An Account Administrator user holds the biggest set of privileges, and is not allowed to modify via current UI, even user try to modify permissions system doesn't support changing for account administrator.

Recover fast in case of a Node failures with ECS HA

When a node is deleted from cloud or made unavailable, it is observed that the it takes more than two minutes until the pods were rescheduled on another node.

It takes some time for the nodes to recover. Failure detection and pod-transitioning are not instantaneous.

CDP Private Cloud Data Services ECS Installation: Failed to perform First Run of services.

If an issue is encountered during the Install Control Plane step of Containerized Cluster First Run, installation will be re-attempted infinitely rather than the command failing.

Since the control plane is installed and uninstalled in a continuous cycle, it is often possible to address the cause of the failure while the command is still running, at which point the next attempted installation should succeed. If this is not successful, abort the First Run command, delete the Containerized Cluster, address the cause of the failure, and retry from the beginning of the Add Cluster wizard. Any nodes that are re-used must be cleaned before re-attempting installation.

Environment creation through the CDP CLI fails when the base cluster includes Ozone

Problem: Attempt to create an environment using the CDP command-line interface fails in a CDP Private Cloud Data Services deployment when the Private Cloud Base cluster is in a degraded state and includes Ozone service.

Workaround: Stopping the Ozone service temporarily in the Private Cloud Base cluster during environment creation prevents the control plane from using Ozone as a logging destination, and avoids this issue.

Filtering the diagnostic data by time range might result in a FileAlreadyExistsException

Problem:Filtering the collected diagnostic data might result in a FileAlreadyExistsException if the /tmp directory already contains a file by that name.

There is currently no workaround for this issue.

Kerberos service does not always handle Cloudera Manager downtime

Problem: The Cloudera Manager Server in the base cluster must be running to generate Kerberos principals for CDP Private Cloud. If there is downtime, you might observe Kerberos-related errors.

Resolve downtime issues on Cloudera Manager. If you encounter Kerberos errors, you can retry the concerned operation such as creating Virtual Warehouses.

Updating user roles for the admin user does not update privileges

In the Management Console, changing roles on the User Management page does not change privileges of the admin user.

None

Upgrade applies values that cannot be patched

If the size of a persistent volume claim in a Containerized Cluster is manually modified, subsequent upgrades of the cluster will fail.

None

Fixed Issues for the CDP Private Cloud Data Services 1.5.4

This section lists the issues that have been fixed since the last release of the CDP Private Cloud Management Console service.

Fixed Issues in Management Console 1.5.4

TSB 2024-746: Concurrent compactions from Spark and modify statements from Hive and Impala can corrupt Iceberg tables.

This issue has been fixed.

TSB 2024-745: Impala returns incorrect results for Iceberg V2 tables when optimized operator is being used in CDW.

This issue has been fixed.

TSB 2024-758: Truncate command on Iceberg V2 branches cause unintentional data deletion.

This issue has been fixed.

OPSX-4446: Duplicate entries in cdp-pvc-truststore

Duplicate certificates are no longer available in the unified truststore.

OPSX-4650: CM - OCP pvc install Wizard - fails if route name is too long

The kubernetes namespace field is limited to 30 characters. This does not affect existing installations.

OPSX-3666: mlx_crud_app DB connection fails with error "unable to create connection: x509: certificate relies on legacy Common Name field, use SANs instead"

If you are upgrading from CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1 or higher versions, and you were previously using an external database, you must regenerate the DB certificate with SAN before upgrading to CDP Private Cloud Data Services 1.5.1 or higher versions.

OPSX-4225: Upgrade failed as cadence pods are crashlooping post upgrade

When doing a fresh install of CDP Private Cloud Data Services 1.5.1, external metadata databases are no longer supported. Instead, the CDP Private Cloud Data Services installer will create an embedded database pod by default, which runs inside the Kubernetes cluster to host the databases required for installation.

If you are upgrading from CDP Private Cloud Data Services 1.4.1 or 1.5.0 to 1.5.1 or higher versions, and you were previously using an external database, you must run the following psql

commands to create the required databases. You should also ensure that the two new databases are owned by the common database users known by the control plane.

```
CREATE DATABASE db-cadence;
CREATE DATABASE db-cadence-visibility;
```

DOCS-19913: OCP upgrade – OCP namespace name must be 29 characters or less

The kubernetes namespace field is limited to 30 characters in OCP. This does not affect existing installations.

COMPX-15475: [CM ECS UPG][150-152] post upgrade prometheus-node-exporter-1.6.0 pod stuck in pending state

Applications, and their pods, that were running before an upgrade are no longer rejected. They get moved to a temporary queue during initialisation if they cannot be placed in the requested queue. This prevents a secondary issue, node rejections, from occurring which caused the pending pods.

OPSAPS-66166: FreeIPA cmadminrole needs more privileges for PvC+ after upgrade

After upgrade, the Cloudera Manager admin role may be missing the Host Administrators privilege in an upgraded cluster.

The cluster administrator should run the following command to manually add this privilege to the role.

```
ipa role-add-privilege <cmadminrole> --privileges="Host Administ
rators"
```

For more information, see Upgrade from 1.5.2 or 1.5.3 to 1.5.4 (ECS).

List of fixed Common Vulnerabilities and Exposures in 1.5.4

Review the Common vulnerabilities and Exposures (CVEs) that were fixed in this release of CDP Private Cloud Data Services.

- CVE-2023-27539: A denial of service vulnerability was found in rubygem-rack in how it parses headers. A carefully crafted input can cause header parsing to take an unexpected amount of time, possibly resulting in a denial of service.
- DSA-5692-1: ghostscript - security update
- CVE-2024-33871: An issue was discovered in Artifex Ghostscript before 10.03.1. contrib/opvp/gdevopvp.c allows arbitrary code execution via a custom Driver library, exploitable via a crafted PostScript document. This occurs because the Driver parameter for opvp (and oprp) devices can have an arbitrary name for a dynamic library; this library is then loaded.
- CVE-2024-33870: An issue was discovered in Artifex Ghostscript before 10.03.1. There is path traversal (via a crafted PostScript document) to arbitrary files if the current directory is in the permitted paths. For example, there can be a transformation of ../../foo to ./../../foo and this will grant access if ./ is permitted.
- CVE-2024-33869: An issue was discovered in Artifex Ghostscript before 10.03.1. Path traversal and command execution can occur (via a crafted PostScript document) because of path reduction in base/gpmisc.c. For example, restrictions on use of %pipe% can be bypassed via the aa/../%pipe%command# output filename.
- CVE-2024-29510: Artifex Ghostscript before 10.03.1 allows memory corruption, and SAFER sandbox bypass, via format string injection with a uniprint device.
- DSA-5679-1: less - security update
- DSA-5682-2: glib2.0 - regression update
- DSA-5682-1: glib2.0 - security update

- CVE-2024-23653: BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. In addition to running containers as build steps, BuildKit also provides APIs for running interactive containers based on built images. It was possible to use these APIs to ask BuildKit to run a container with elevated privileges. Normally, running such containers is only allowed if special `security.insecure` entitlement is enabled both by buildkitd configuration and allowed by the user initializing the build request. The issue has been fixed in v0.12.5. Avoid using BuildKit frontends from untrusted sources.
- CVE-2024-23652: BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. A malicious BuildKit frontend or Dockerfile using `RUN --mount` could trick the feature that removes empty files created for the mountpoints into removing a file outside the container, from the host system. The issue has been fixed in v0.12.5. Workarounds include avoiding using BuildKit frontends from an untrusted source or building an untrusted Dockerfile containing `RUN --mount` feature.
- CVE-2023-36665: protobuf.js (aka protobufjs) 6.10.0 through 7.x before 7.2.5 allows Prototype Pollution, a different vulnerability than CVE-2022-25878. A user-controlled protobuf message can be used by an attacker to pollute the prototype of Object.prototype by adding and overwriting its data and functions. Exploitation can involve: (1) using the function parse to parse protobuf messages on the fly, (2) loading .proto files by using load/loadSync functions, or (3) providing untrusted input to the functions ReflectionObject.setParsedOption and util.setProperty.
- CVE-2024-22682: DuckDB <=0.9.2 and DuckDB extension-template <=0.9.2 are vulnerable to malicious extension injection via the custom extension feature.
- CVE-2022-30123: A sequence injection vulnerability exists in Rack <2.0.9.1, <2.1.4.1 and <2.2.3.1 which could allow is a possible shell escape in the Lint and CommonLogger components of Rack.
- CVE-2023-38545: This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake. When curl is asked to pass along the hostname to the SOCKS5 proxy to allow that to resolve the address instead of it getting done by curl itself, the maximum length that hostname can be is 255 bytes. If the hostname is detected to be longer than 255 bytes, curl switches to local name resolving and instead passes on the resolved address only to the proxy. Due to a bug, the local variable that means 'let the host resolve the name' could get the wrong value during a slow SOCKS5 handshake, and contrary to the intention, copy the too long hostname to the target buffer instead of copying just the resolved address there.
- CVE-2023-32002: The use of `Module._load()` can bypass the policy mechanism and require modules outside of the policy.json definition for a given module. This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.
- CVE-2016-5397: The Apache Thrift Go client library exposed the potential during code generation for command injection due to using an external formatting tool. Affected Apache Thrift 0.9.3 and older, Fixed in Apache Thrift 0.10.0.
- CVE-2022-3294: Users may have access to secure endpoints in the control plane network. Kubernetes clusters are only affected if an untrusted user can modify Node objects and send proxy requests to them. Kubernetes supports node proxying, which allows clients of kube-apiserver to access endpoints of a Kubelet to establish connections to Pods, retrieve container logs, and more. While Kubernetes already validates the proxying address for Nodes, a bug in kube-apiserver made it possible to bypass this validation. Bypassing this validation could allow authenticated requests destined for Nodes to to the API server's private network.
- CVE-2023-46402: git-urls 1.0.0 allows ReDOS (Regular Expression Denial of Service) in urls.go.
- RHSA-2024:2098: The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.
- RHSA-2024:0752: The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.
- CVE-2024-23651: BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. Two malicious build steps running in parallel sharing the same cache mounts with subpaths could cause a race condition that can lead to files from the host system being accessible to the build container. The issue has been fixed in v0.12.5. Workarounds include, avoiding using BuildKit frontend from an untrusted source or building an untrusted Dockerfile containing cache mounts with --mount=type=cache,source=... options.
- RHSA-2023:4419: OpenSSH is an SSH protocol implementation supported by a number of Linux, UNIX, and similar operating systems. It includes the core files necessary for both the OpenSSH client and server.

- RHSA-2024:2699: Git Large File Storage (LFS) replaces large files such as audio samples, videos, datasets, and graphics with text pointers inside Git, while storing the file contents on a remote server.
- RHSA-2024:1444: Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- RHSA-2023:5360: Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- RHSA-2023:5850: Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- CVE-2023-43646: get-func-name is a module to retrieve a function's name securely and consistently both in NodeJS and the browser. Versions prior to 2.0.1 are subject to a regular expression denial of service (redos) vulnerability which may lead to a denial of service when parsing malicious input. This vulnerability can be exploited when there is an imbalance in parentheses, which results in excessive backtracking and subsequently increases the CPU load and processing time significantly. This vulnerability can be triggered using the following input: '\t'.repeat(54773) + '\t/function/i'. This issue has been addressed in commit `f934b228b` which has been included in releases from 2.0.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.
- CVE-2023-45133: Babel is a compiler for writingJavaScript. In `@babel/traverse` prior to versions 7.23.2 and 8.0.0-alpha.4 and all versions of `babel-traverse`, using Babel to compile code that was specifically crafted by an attacker can lead to arbitrary code execution during compilation, when using plugins that rely on the `path.evaluate()`or `path.evaluateTruthy()` internal Babel methods. Known affected plugins are `@babel/plugin-transform-runtime`; `@babel/preset-env` when using its `useBuiltIns` option; and any "polyfill provider" plugin that depends on `@babel/helper-define-polyfill-provider`, such as `babel-plugin-polyfill-corejs3`, `babel-plugin-polyfill-corejs2`, `babel-plugin-polyfill-es-shims`, `babel-plugin-polyfill-regenerator`. No other plugins under the `@babel/` namespace are impacted, but third-party plugins might be. Users that only compile trusted code are not impacted. The vulnerability has been fixed in `@babel/traverse@7.23.2` and `@babel/traverse@8.0.0-alpha.4`. Those who cannot upgrade `@babel/traverse` and are using one of the affected packages mentioned above should upgrade them to their latest version to avoid triggering the vulnerable code path in affected `@babel/traverse` versions: `@babel/plugin-transform-runtime` v7.23.2, `@babel/preset-env` v7.23.2, `@babel/helper-define-polyfill-provider` v0.4.3, `babel-plugin-polyfill-corejs2` v0.4.6, `babel-plugin-polyfill-corejs3` v0.8.5, `babel-plugin-polyfill-es-shims` v0.10.0, `babel-plugin-polyfill-regenerator` v0.5.3.
- CVE-2024-27983: An attacker can make the Node.js HTTP/2 server completely unavailable by sending a small amount of HTTP/2 frames packets with a few HTTP/2 frames inside. It is possible to leave some data in nghttp2 memory after reset when headers with HTTP/2 CONTINUATION frame are sent to the server and then a TCP connection is abruptly closed by the client triggering the Http2Session destructor while header frames are still being processed (and stored in memory) causing a race condition.
- CVE-2021-33910: basic/unit-name.c in systemd prior to 246.15, 247.8, 248.5, and 249.1 has a Memory Allocation with an Excessive Size Value (involving strdupa and alloca for a pathname controlled by a local attacker) that results in an operating system crash.
- CVE-2023-43665: In Django 3.2 before 3.2.22, 4.1 before 4.1.12, and 4.2 before 4.2.6, the django.utils.text.Truncator chars() and words() methods (when used with html=True) are subject to a potential DoS (denial of service) attack via certain inputs with very long, potentially malformed HTML text. The chars() and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which are thus also vulnerable. NOTE: this issue exists because of an incomplete fix for CVE-2019-14232.
- CVE-2023-46695: An issue was discovered in Django 3.2 before 3.2.23, 4.1 before 4.1.13, and 4.2 before 4.2.7. The NFKC normalization is slow on Windows. As a consequence, django.contrib.auth.forms.UsernameField is subject to a potential DoS (denial of service) attack via certain inputs with a very large number of Unicode characters.
- CVE-2023-41164: In Django 3.2 before 3.2.21, 4.1 before 4.1.11, and 4.2 before 4.2.5, django.utils.encoding.uri_to_iri() is subject to a potential DoS (denial of service) attack via certain inputs with a very large number of Unicode characters.
- CVE-2024-24680: An issue was discovered in Django 3.2 before 3.2.24, 4.2 before 4.2.10, and Django 5.0 before 5.0.2. The intcomma template filter was subject to a potential denial-of-service attack when used with very long strings.
- CVE-2022-44570: A denial of service vulnerability in the Range header parsing component of Rack >= 1.5.0. A Carefully crafted input can cause the Range header parsing component in Rack to take an unexpected amount of

time, possibly resulting in a denial of service attack vector. Any applications that deal with Range requests (such as streaming applications, or applications that serve files) may be impacted.

- CVE-2023-27530: A DoS vulnerability exists in Rack <v3.0.4.2, <v2.2.6.3, <v2.1.4.3 and <v2.0.9.3 within in the Multipart MIME parsing code in which could allow an attacker to craft requests that can be abuse to cause multipart parsing to take longer than expected.
- CVE-2022-44571: There is a denial of service vulnerability in the Content-Disposition parsingcomponent of Rack fixed in 2.0.9.2, 2.1.4.2, 2.2.4.1, 3.0.0.1. This could allow an attacker to craft an input that can cause Content-Disposition header parsing in Rackto take an unexpected amount of time, possibly resulting in a denial ofservice attack vector. This header is used typically used in multipartparsing. Any applications that parse multipart posts using Rack (virtuallyall Rails applications) are impacted.
- CVE-2020-8184: A reliance on cookies without validation/integrity check security vulnerability exists in rack < 2.2.3, rack < 2.1.4 that makes it is possible for an attacker to forge a secure or host-only cookie prefix.
- CVE-2022-44572: A denial of service vulnerability in the multipart parsing component of Rack fixed in 2.0.9.2, 2.1.4.2, 2.2.4.1 and 3.0.0.1 could allow an attacker tocraft input that can cause RFC2183 multipart boundary parsing in Rack to take an unexpected amount of time, possibly resulting in a denial of service attack vector. Any applications that parse multipart posts using Rack (virtually all Rails applications) are impacted.
- CVE-2022-30122: A possible denial of service vulnerability exists in Rack <2.0.9.1, <2.1.4.1 and <2.2.3.1 in the multipart parsing component of Rack.
- CVE-2023-28319: A use after free vulnerability exists in curl <v8.1.0 in the way libcurl offers a feature to verify an SSH server's public key using a SHA 256 hash. When this check fails, libcurl would free the memory for the fingerprint before it returns an error message containing the (now freed) hash. This flaw risks inserting sensitive heap-based data into the error message that might be shown to users or otherwise get leaked and revealed.
- CVE-2023-35945: Envoy is a cloud-native high-performance edge/middle/service proxy. Envoy’s HTTP/2 codec may leak a header map and bookkeeping structures upon receiving `RST_STREAM` immediately followed by the `GOAWAY` frames from an upstream server. In nghttp2, cleanup of pending requests due to receipt of the `GOAWAY` frame skips de-allocation of the bookkeeping structure and pending compressed header. The error return [code path] is taken if connection is already marked for not sending more requests due to `GOAWAY` frame. The clean-up code is right after the return statement, causing memory leak. Denial of service through memory exhaustion. This vulnerability was patched in versions(s) 1.26.3, 1.25.8, 1.24.9, 1.23.11.
- RHSA-2023:4035: Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- RHSA-2023:5362: Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- RHSA-2023:5869: Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- RHSA-2024:1435: PostgreSQL is an advanced object-relational database management system. The postgresql-jdbc package includes the .jar files needed for Java programs to access a PostgreSQL database.
- CVE-2024-23226: The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, tvOS 17.4. Processing web content may lead to arbitrary code execution.
- CVE-2023-42950: A use after free issue was addressed with improved memory management. This issue is fixed in Safari 17.2, iOS 17.2 and iPadOS 17.2, tvOS 17.2, watchOS 10.2, macOS Sonoma 14.2. Processing maliciously crafted web content may lead to arbitrary code execution.
- RHSA-2024:2126: WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform.
- CVE-2023-30608: sqlparse is a non-validating SQL parser module for Python. In affected versions the SQL parser contains a regular expression that is vulnerable to ReDoS (Regular Expression Denial of Service). This issue was introduced by commit `e75e358`. The vulnerability may lead to Denial of Service (DoS). This issues has been fixed in sqlparse 0.4.4 by commit `c457abd5f`. Users are advised to upgrade. There are no known workarounds for this issue.
- CVE-2023-6932: A use-after-free vulnerability in the Linux kernel's ipv4: igmp component can be exploited to achieve local privilege escalation. A race condition can be exploited to cause a timer be mistakenly registered on a RCU read locked object which is freed by another thread. We recommend upgrading past commit e2b706c691905fe78468c361aaabc719d0a496f1.

- CVE-2023-6931: A heap out-of-bounds write vulnerability in the Linux kernel's Performance Events system component can be exploited to achieve local privilege escalation. A perf_event's read_size can overflow, leading to an heap out-of-bounds increment or write in perf_read_group(). We recommend upgrading past commit 382c27f4ed28f803b1f1473ac2d8db0afc795a1b.
- CVE-2023-20588: A division-by-zero error on some AMD processors can potentially return speculative data resulting in loss of confidentiality.
- CVE-2023-40590: GitPython is a python library used to interact with Git repositories. When resolving a program, Python/Windows look for the current working directory, and after that the PATH environment. GitPython defaults to use the `git` command, if a user runs GitPython from a repo has a `git.exe` or `git` executable, that program will be run instead of the one in the user's `PATH`. This is more of a problem on how Python interacts with Windows systems, Linux and any other OS aren't affected by this. But probably people using GitPython usually run it from the CWD of a repo. An attacker can trick a user to download a repository with a malicious `git` executable, if the user runs/imports GitPython from that directory, it allows the attacker to run any arbitrary commands. There is no fix currently available for windows users, however there are a few mitigations. 1: Default to an absolute path for the git program on Windows, like `C:\\Program Files\\Git\\cmd\\git.EXE` (default git path installation). 2: Require users to set the `GIT_PYTHON_GIT_EXECUTABLE` environment variable on Windows systems. 3: Make this problem prominent in the documentation and advise users to never run GitPython from an untrusted repo, or set the `GIT_PYTHON_GIT_EXECUTABLE` env var to an absolute path. 4: Resolve the executable manually by only looking into the `PATH` environment variable.
- CVE-2023-32559: A privilege escalation vulnerability exists in the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. The use of the deprecated API `process.binding()` can bypass the policy mechanism by requiring internal modules and eventually take advantage of `process.binding('spawn_sync')` run arbitrary code, outside of the limits defined in a `policy.json` file. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.
- CVE-2023-32006: The use of `module.constructor.createRequire()` can bypass the policy mechanism and require modules outside of the policy.json definition for a given module. This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x, and, 20.x. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.
- CVE-2023-30585: A vulnerability has been identified in the Node.js (.msi version) installation process, specifically affecting Windows users who install Node.js using the .msi installer. This vulnerability emerges during the repair operation, where the ""msiexec.exe"" process, running under the NT AUTHORITY\SYSTEM context, attempts to read the %USERPROFILE% environment variable from the current user's registry.

  The issue arises when the path referenced by the %USERPROFILE% environment variable does not exist. In such cases, the ""msiexec.exe"" process attempts to create the specified path in an unsafe manner, potentially leading to the creation of arbitrary folders in arbitrary locations.

  The severity of this vulnerability is heightened by the fact that the %USERPROFILE% environment variable in the Windows registry can be modified by standard (or ""non-privileged"") users. Consequently, unprivileged actors, including malicious entities or trojans, can manipulate the environment variable key to deceive the privileged ""msiexec.exe"" process. This manipulation can result in the creation of folders in unintended and potentially malicious locations.

  It is important to note that this vulnerability is specific to Windows users who install Node.js using the .msi installer. Users who opt for other installation methods are not affected by this particular issue.
- CVE-2023-4807: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.

  The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.

  The consequences of this kind of internal application state corruption canbe various - from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the

worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.

The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.

As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- CVE-2023-40283: An issue was discovered in l2cap_sock_release in net/bluetooth/l2cap_sock.c in the Linux kernel before 6.4.10. There is a use-after-free because the children of an sk are mishandled.
- CVE-2023-42752: An integer overflow flaw was found in the Linux kernel. This issue leads to the kernel allocating `skb_shared_info` in the userspace, which is exploitable in systems without SMAP protection since `skb_shared_info` contains references to function pointers.
- CVE-2023-1436: An infinite recursion is triggered in Jettison when constructing a JSONArray from a Collection that contains a self-reference in one of its elements. This leads to a StackOverflowError exception being thrown.
- CVE-2022-40149: Those using Jettison to parse untrusted XML or JSON data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack.
- CVE-2022-40150: Those using Jettison to parse untrusted XML or JSON data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by Out of memory. This effect may support a denial of service attack.
- CVE-2022-45685: A stack overflow in Jettison before v1.5.2 allows attackers to cause a Denial of Service (DoS) via crafted JSON data.
- CVE-2022-45693: Jettison before v1.5.2 was discovered to contain a stack overflow via the map parameter. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.
- RHSA-2024:2447: OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library.
- CVE-2020-29562: The iconv function in the GNU C Library (aka glibc or libc6) 2.30 to 2.32, when converting UCS4 text containing an irreversible character, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.
- CVE-2021-27645: The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.
- CVE-2020-12723: regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.
- CVE-2020-10878: Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.
- CVE-2020-10543: Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
- CVE-2021-20232: A flaw was found in gnutls. A use after free issue in client_send_params in lib/ext/pre_shared_key.c may lead to memory corruption and other potential consequences.
- CVE-2021-20231: A flaw was found in gnutls. A use after free issue in client sending key_share extension may lead to memory corruption and other consequences.
- CVE-2023-38546: This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of conditions are met. libcurl performs transfers. In its API, an application creates 'easy handles' that are the individual handles for single transfers. libcurl provides a function call that duplicates an easy handle called curl_easy_duphandle. If a transfer has cookies enabled when the handle is duplicated, the cookie-enable state is also cloned - but without cloning the actual cookies. If the source handle did not read any cookies from

a specific file on disk, the cloned version of the handle would instead store the file name as none (using the four ASCII letters, no quotes).Subsequent use of the cloned handle that does not explicitly set a source to load cookies from would then inadvertently load cookies from a file named none - if such a file exists and is readable in the current directory of the program using libcurl. And if using the correct file format of course.

- CVE-2017-7244: The _pcre32_xclass function in pcre_xclass.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (invalid memory read) via a crafted file.
- CVE-2018-16429: GNOME GLib 2.56.1 has an out-of-bounds read vulnerability in g_markup_parse_context_parse() in gmarkup.c, related to utf8_str().
- CVE-2019-13012: The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.60.0 creates directories using g_file_make_directory_with_parents (kfsb->dir, NULL, NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used; for files, default file permissions are used. This is similar to CVE-2019-12450.
- CVE-2021-28153: An issue was discovered in GNOME GLib before 2.66.8. When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.)
- CVE-2023-2602: A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create() to return an error, which can exhaust the process memory.
- CVE-2015-2059: The stringprep_utf8_to_ucs4 function in libin before 1.31, as used in jabberd2, allows context-dependent attackers to read system memory and possibly have other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read.
- CVE-2015-8948: idn in GNU libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read.
- CVE-2017-5969: libxml2 2.9.4, when used in recover mode, allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted XML document. NOTE: The maintainer states "I would disagree of a CVE with the Recover parsing option which should only be used for manual recovery at least for XML parser.
- CVE-2017-8872: The htmlParseTryOrFinish function in HTMLparser.c in libxml2 2.9.4 allows attackers to cause a denial of service (buffer over-read) or information disclosure.
- CVE-2017-9048: libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a stack-based buffer overflow. The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. At the end of the routine, the function may strcat two more characters without checking whether the current strlen(buf) + 2 < size. This vulnerability causes programs that use libxml2, such as PHP, to crash.
- CVE-2016-4984: /usr/libexec/openldap/generate-server-cert.sh in openldap-servers sets weak permissions for the TLS certificate, which allows local users to obtain the TLS certificate by leveraging a race condition between the creation of the certificate, and the chmod to protect it.
- CVE-2017-11462: Double free vulnerability in MIT Kerberos 5 (aka krb5) allows attackers to have unspecified impact via vectors involving automatic deletion of security contexts on error.
- CVE-2016-8621: The `curl_getdate` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an input with one digit short.
- CVE-2016-8622: The URL percent-encoding decode function in libcurl before 7.51.0 is called `curl_easy_unescape`. Internally, even if this function would be made to allocate a unscape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.
- CVE-2016-8623: A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use-after-free leading to information disclosure.
- CVE-2021-3200: Buffer overflow vulnerability in libsolv 2020-12-13 via the Solver * testcase_read(Pool *pool, FILE *fp, const char *testcase, Queue *job, char **resultp, int *resultflagsp function at src/testcase.c: line 2334, which could cause a denial of service

- CVE-2016-9586: curl before version 7.52.0 is vulnerable to a buffer overflow when doing a large floating point output in libcurl's implementation of the printf() functions. If there are any application that accepts a format string from the outside without necessary input filtering, it could allow remote attacks.
- CVE-2017-1000100: When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about 515 bytes), the file name is truncated to fit within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length. This too large value is then used in the sendto() call, making curl attempt to send more data than what is actually put into the buffer. The endto() function will then read beyond the end of the heap based buffer. A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client hasn't restricted which protocols it allows redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protocols with --proto-redir and libcurl's with CURLOPT_REDIR_PROTOCOLS.
- CVE-2021-37621: Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop was found in Exiv2 versions v0.27.4 and earlier. The infinite loop is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the image ICC profile, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p C`). The bug is fixed in version v0.27.5.
- CVE-2021-37620: Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.4 and earlier. The out-of-bounds read is triggered when Exiv2 is used to read the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.5.
- CVE-2021-37616: Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A null pointer dereference was found in Exiv2 versions v0.27.4 and earlier. The null pointer dereference is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the interpreted (translated) data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p t` or `-P t`). The bug is fixed in version v0.27.5.
- CVE-2021-34335: Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A floating point exception (FPE) due to an integer divide by zero was found in Exiv2 versions v0.27.4 and earlier. The FPE is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the interpreted (translated) data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p t` or `-P t`). The bug is fixed in version v0.27.5.
- CVE-2021-37623: Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop was found in Exiv2 versions v0.27.4 and earlier. The infinite loop is triggered when Exiv2 is used to modify the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when deleting the IPTC data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-d I rm`). The bug is fixed in version v0.27.5.
- CVE-2021-34334: Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop is triggered when Exiv2 is used to read the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.5.
- CVE-2021-32815: Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. The assertion failure is triggered when Exiv2 is used to modify the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when modifying the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `fi`. ### Patches The bug is fixed in version v0.27.5. ### References Regression test and bug fix: #1739 ### For more information Please see our security policy for information about Exiv2 security.

- CVE-2021-37622: Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop was found in Exiv2 versions v0.27.4 and earlier. The infinite loop is triggered when Exiv2 is used to modify the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when deleting the IPTC data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-d I rm`). The bug is fixed in version v0.27.5.
- CVE-2020-18771: Exiv2 0.27.99.0 has a global buffer over-read in Exiv2::Internal::Nikon1MakerNote::print0x0088 in nikonmn_int.cpp which can result in an information leak.
- CVE-2021-37615: Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A null pointer dereference was found in Exiv2 versions v0.27.4 and earlier. The null pointer dereference is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the interpreted (translated) data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p t` or `-P t`). The bug is fixed in version v0.27.5.
- CVE-2018-13419: An issue has been found in libsndfile 1.0.28. There is a memory leak in psf_allocate in common.c, as demonstrated by sndfile-convert. NOTE: The maintainer and third parties were unable to reproduce and closed the issue
- CVE-2023-4132: A use-after-free vulnerability was found in the siano smsusb module in the Linux kernel. The bug occurs during device initialization when the siano device is plugged in. This flaw allows a local user to crash the system, causing a denial of service condition.
- CVE-2021-41617: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.
- CVE-2023-35827: An issue was discovered in the Linux kernel through 6.3.8. A use-after-free was found in ravb_remove in drivers/net/ethernet/renesas/ravb_main.c.
- CVE-2023-3212: A NULL pointer dereference issue was found in the gfs2 file system in the Linux kernel. It occurs on corrupt gfs2 file systems when the evict code tries to reference the journal descriptor structure after it has been freed and set to NULL. A privileged local user could use this flaw to cause a kernel panic.
- CVE-2022-3162: Users authorized to list or watch one type of namespaced custom resource cluster-wide can read custom resources of a different type in the same API group without authorization. Clusters are impacted by this vulnerability if all of the following are true: 1. There are 2+ CustomResourceDefinitions sharing the same API group 2. Users have cluster-wide list or watch authorization on one of those custom resources. 3. The same users are not authorized to read another custom resource in the same API group.
- RHSA-2023:3042: GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language (elisp), and the capability to read e-mail and news.
- RHSA-2024:0606: OpenSSH is an SSH protocol implementation supported by a number of Linux, UNIX, and similar operating systems. It includes the core files necessary for both the OpenSSH client and server.
- CVE-2024-23650: BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. A malicious BuildKit client or frontend could craft a request that could lead to BuildKit daemon crashing with a panic. The issue has been fixed in v0.12.5. As a workaround, avoid using BuildKit frontends from untrusted sources.
- RHSA-2023:2758: The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.
- RHSA-2023:6939: The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.
- RHSA-2023:2866: Git Large File Storage (LFS) replaces large files such as audio samples, videos, datasets, and graphics with text pointers inside Git, while storing the file contents on a remote server.

- CVE-2024-22025: A vulnerability in Node.js has been identified, allowing for a Denial of Service (DoS) attack through resource exhaustion when using the fetch() function to retrieve content from an untrusted URL.

  The vulnerability stems from the fact that the fetch() function in Node.js always decodes Brotli, making it possible for an attacker to cause resource exhaustion when fetching content from an untrusted URL.

  An attacker controlling the URL passed into fetch() can exploit this vulnerability to exhaust memory, potentially leading to process termination, depending on the system configuration.
- CVE-2022-29244: npm pack ignores root-level .gitignore and .npmignore file exclusion directives when run in a workspace or with a workspace flag (ie. `--workspaces`, `--workspace=<name>`). Anyone who has run `npm pack` or `npm publish` inside a workspace, as of v7.9.0 and v7.13.0 respectively, may be affected and have published files into the npm registry they did not intend to include. Users should upgrade to the latest, patched version of npm v8.11.0, run: npm i -g npm@latest . Node.js versions v16.15.1, v17.19.1, and v18.3.0 include the patched v8.11.0 version of npm.
- CVE-2023-46809: A flaw was found in Node.js. The privateDecrypt() API of the crypto library may allow a covert timing side-channel during PKCS#1 v1.5 padding error handling. This issue revealed significant timing differences in decryption for valid and invalid ciphertexts, which may allow a remote attacker to decrypt captured RSA ciphertexts or forge signatures, especially in scenarios involving API endpoints processing JSON Web Encryption messages.
- CVE-2024-27982: The team has identified a critical vulnerability in the http server of the most recent version of Node, where malformed headers can lead to HTTP request smuggling. Specifically, if a space is placed before a content-length header, it is not interpreted correctly, enabling attackers to smuggle in a second request within the body of the first.
- CVE-2024-29041: Express.js minimalist web framework for node. Versions of Express.js prior to 4.19.0 and all pre-release alpha and beta versions of 5.0 are affected by an open redirect vulnerability using malformed URLs. When a user of Express performs a redirect using a user-provided URL Express performs an encode [using `encodeurl`](https://github.com/pillarjs/encodeurl) on the contents before passing it to the `location` header. This can cause malformed URLs to be evaluated in unexpected ways by common redirect allow list implementations in Express applications, leading to an Open Redirect via bypass of a properly implemented allow list. The main method impacted is `res.location()` but this is also called from within `res.redirect()`. The vulnerability is fixed in 4.19.2 and 5.0.0-beta.3.
- RHSA-2023:7747: The libxml2 library is a development toolbox providing the implementation of various XML standards.
- RHSA-2024:0463: The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.
- RHSA-2024:0465: SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server.
- RHSA-2024:2438: Pluggable Authentication Modules (PAM) provide a system to set up authentication policies without the need to recompile programs to handle authentication.
- CVE-2020-29363: An issue was discovered in p11-kit 0.23.6 through 0.23.21. A heap-based buffer overflow has been discovered in the RPC protocol used by p11-kit server/remote commands and the client library. When the remote entity supplies a serialized byte array in a CK_ATTRIBUTE, the receiving entity may not allocate sufficient length for the buffer to store the deserialized value.
- CVE-2020-27350: APT had several integer overflows and underflows while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in files apt-pkg/contrib/extracttar.cc, apt-pkg/deb/debfile.cc, and apt-pkg/contrib/arfile.cc. This issue affects: apt 1.2.32ubuntu0 versions prior to 1.2.32ubuntu0.2; 1.6.12ubuntu0 versions prior to 1.6.12ubuntu0.2; 2.0.2ubuntu0 versions prior to 2.0.2ubuntu0.2; 2.1.10ubuntu0 versions prior to 2.1.10ubuntu0.1;
- CVE-2020-24659: An issue was discovered in GnuTLS before 3.6.15. A server can trigger a NULL pointer dereference in a TLS 1.3 client if a no_renegotiation alert is sent with unexpected timing, and then an invalid second handshake occurs. The crash happens in the application's error handling path, where the gnutls_deinit function is called after detecting a handshake failure.

- CVE-2023-32360: An authentication issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4. An unauthenticated user may be able to access recently printed documents.
- CVE-2023-34241: OpenPrinting CUPS is a standards-based, open source printing system for Linux and other Unix-like operating systems. Starting in version 2.0.0 and prior to version 2.4.6, CUPS logs data of free memory to the logging service AFTER the connection has been closed, when it should have logged the data right before. This is a use-after-free bug that impacts the entire cupsd process.

  The exact cause of this issue is the function `httpClose(con->http)` being called in `scheduler/client.c`. The problem is that httpClose always, provided its argument is not null, frees the pointer at the end of the call, only for cupsdLogClient to pass the pointer to httpGetHostname. This issue happens in function `cupsdAcceptClient` if LogLevel is warn or higher and in two scenarios: there is a double-lookup for the IP Address (HostNameLookups Double is set in `cupsd.conf`) which fails to resolve, or if CUPS is compiled with TCP wrappers and the connection is refused by rules from `/etc/hosts.allow` and `/etc/hosts.deny`.

  Version 2.4.6 has a patch for this issue.
- CVE-2021-3995: A logic error was found in the libmount library of util-linux in the function that allows an unprivileged user to unmount a FUSE filesystem. This flaw allows an unprivileged local attacker to unmount FUSE filesystems that belong to certain other users who have a UID that is a prefix of the UID of the attacker in its string form. An attacker may use this flaw to cause a denial of service to applications that use the affected filesystems.
- CVE-2021-3996: A logic error was found in the libmount library of util-linux in the function that allows an unprivileged user to unmount a FUSE filesystem. This flaw allows a local user on a vulnerable system to unmount other users' filesystems that are either world-writable themselves (like /tmp) or mounted in a world-writable directory. An attacker may use this flaw to cause a denial of service to applications that use the affected filesystems.
- CVE-2023-3138: A vulnerability was found in libX11. The security flaw occurs because the functions in src/InitExt.c in libX11 do not check that the values provided for the Request, Event, or Error IDs are within the bounds of the arrays that those functions write to, using those IDs as array indexes. They trust that they were called with values provided by an Xserver adhering to the bounds specified in the X11 protocol, as all X servers provided by X.Org do. As the protocol only specifies a single byte for these values, an out-of-bounds value provided by a malicious server (or a malicious proxy-in-the-middle) can only overwrite other portions of the Display structure and not write outside the bounds of the Display structure itself, possibly causing the client to crash with this memory corruption.
- CVE-2021-20305: A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalers, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation. The highest threat to this vulnerability is to confidentiality, integrity, as well as system availability.
- CVE-2021-3580: A flaw was found in the way nettle's RSA decryption functions handled specially crafted ciphertext. An attacker could use this flaw to provide a manipulated ciphertext leading to application crash and denial of service.
- CVE-2021-24031: In the Zstandard command-line utility prior to v1.4.1, output files were created with default permissions. Correct file permissions (matching the input) would only be set at completion time. Output files could therefore be readable or writable to unintended parties.
- CVE-2023-22045: Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code

that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).

- CVE-2023-22049: Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
- RHSA-2023:7034: Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems.
- CVE-2023-49081: aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Improper validation made it possible for an attacker to modify the HTTP request (e.g. to insert a new header) or create a new HTTP request if the attacker controls the HTTP version. The vulnerability only occurs if the attacker can control the HTTP version of the request. This issue has been patched in version 3.9.0.
- CVE-2024-23829: aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Security-sensitive parts of the Python HTTP parser retained minor differences in allowable character sets, that must trigger error handling to robustly match frame boundaries of proxies in order to protect against injection of additional requests. Additionally, validation could trigger exceptions that were not handled consistently with processing of other malformed input. Being more lenient than internet standards require could, depending on deployment environment, assist in request smuggling. The unhandled exception could cause excessive resource consumption on the application server and/or its logging facilities. This vulnerability exists due to an incomplete fix for CVE-2023-47627. Version 3.9.2 fixes this vulnerability.
- CVE-2023-49082: aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Improper validation makes it possible for an attacker to modify the HTTP request (e.g. insert a new header) or even create a new HTTP request if the attacker controls the HTTP method. The vulnerability occurs only if the attacker can control the HTTP method (GET, POST etc.) of the request. If the attacker can control the HTTP version of the request it will be able to modify the request (request smuggling). This issue has been patched in version 3.9.0.
- CVE-2024-25629: c-ares is a C library for asynchronous DNS requests. `ares__read_line()` is used to parse local configuration files such as `/etc/resolv.conf`, `/etc/nsswitch.conf`, the `HOSTALIASES` file, and if using a c-ares version prior to 1.27.0, the `/etc/hosts` file. If any of these configuration files has an embedded `NULL` character as the first character in a new line, it can lead to attempting to read memory prior to the start of the given buffer which may result in a crash. This issue is fixed in c-ares 1.27.0. No known workarounds exist.
- CVE-2023-23916: An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors.
- CVE-2023-27537: A double free vulnerability exists in libcurl <8.0.0 when sharing HSTS data between separate "handles". This sharing was introduced without considerations for do this sharing across separate threads but there was no indication of this fact in the documentation. Due to missing mutexes or thread locks, two threads sharing the same HSTS data could end up doing a double-free or use-after-free.
- CVE-2018-1002104: Versions < 1.5 of the Kubernetes ingress default backend, which handles invalid ingress traffic, exposed prometheus metrics publicly.
- DSA-5686-1: dav1d - security update
- RHSA-2024:1530: Expat is a C library for parsing XML documents.

- RHSA-2023:1583: Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- RHSA-2023:4536: Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language.
- RHSA-2022:1830: PostgreSQL is an advanced object-relational database management system (DBMS).
- CVE-2021-3782: An internal reference count is held on the buffer pool, incremented every time a new buffer is created from the pool. The reference count is maintained as an int; on LP64 systems this can cause the reference count to overflow if the client creates a large number of wl_shm buffer objects, or if it can coerce the server to create a large number of external references to the buffer storage. With the reference count overflowing, a use-after-free can be constructed on the wl_shm_pool tracking structure, where values may be incremented or decremented; it may also be possible to construct a limited oracle to leak 4 bytes of server-side memory to the attacking client at a time.
- CVE-2020-36023: An issue was discovered in freedesktop poppler version 20.12.1, allows remote attackers to cause a denial of service (DoS) via crafted .pdf file to FoFiType1C::cvtGlyph function.
- CVE-2020-36024: An issue was discovered in freedesktop poppler version 20.12.1, allows remote attackers to cause a denial of service (DoS) via crafted .pdf file to FoFiType1C::convertToType1 function.
- CVE-2022-37050: In Poppler 22.07.0, PDFDoc::savePageAs in PDFDoc.c callows attackers to cause a denial-of-service (application crashes with SIGABRT) by crafting a PDF file in which the xref data structure is mishandled in getCatalog processing. Note that this vulnerability is caused by the incomplete patch of CVE-2018-20662.
- CVE-2022-37051: An issue was discovered in Poppler 22.07.0. There is a reachable abort which leads to denial of service because the main function in pdfunite.cc lacks a stream check before saving an embedded file.
- CVE-2022-37052: A reachable Object::getString assertion in Poppler 22.07.0 allows attackers to cause a denial of service due to a failure in markObject.
- RHSA-2024:2302: GStreamer is a streaming media framework based on graphs of filters which operate on media data. The gstreamer1-plugins-base packages contain a collection of well-maintained base plug-ins.
- RHSA-2024:2295: The libjpeg-turbo packages contain a library of functions for manipulating JPEG images. They also contain simple client programs for accessing the libjpeg functions. These packages provide the same functionality and API as libjpeg but with better performance.
- RHSA-2024:2184: libsndfile is a C library for reading and writing files containing sampled sound, such as AIFF, AU, or WAV.
- RHSA-2024:2410: HarfBuzz is an implementation of the OpenType Layout engine.
- CVE-2023-42843: An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1, Safari 17.1, macOS Sonoma 14.1. Visiting a malicious website may lead to address bar spoofing.
- CVE-2023-42956: The issue was addressed with improved memory handling. This issue is fixed in Safari 17.2, iOS 17.2 and iPadOS 17.2, macOS Sonoma 14.2. Processing web content may lead to a denial-of-service.
- CVE-2024-23252: Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
- CVE-2024-23254: The issue was addressed with improved UI handling. This issue is fixed in tvOS 17.4, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, Safari 17.4. A malicious website may exfiltrate audio data cross-origin.
- CVE-2024-23263: A logic issue was addressed with improved validation. This issue is fixed in tvOS 17.4, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, Safari 17.4. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.
- CVE-2024-23280: An injection issue was addressed with improved validation. This issue is fixed in Safari 17.4, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, watchOS 10.4, tvOS 17.4. A maliciously crafted webpage may be able to fingerprint the user.
- CVE-2024-23284: A logic issue was addressed with improved state management. This issue is fixed in tvOS 17.4, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, Safari 17.4. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.
- RHSA-2024:2145: The libX11 packages contain the core X11 protocol client library.

- RHSA-2024:2433: Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zero Configuration Networking. It facilitates service discovery on a local network. Avahi and Avahi-aware applications allow you to plug your computer into a network and, with no configuration, view other people to chat with, view printers to print with, and find shared files on other computers.
- RHSA-2024:2289: The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.
- RHSA-2023:2867: PostgreSQL is an advanced object-relational database management system. The postgresql-jdbc package includes the .jar files needed for Java programs to access a PostgreSQL database.
- CVE-2022-21724: pgjdbc is the offical PostgreSQL JDBC Driver. A security hole was found in the jdbc driver for postgresql database while doing security research. The system using the postgresql library will be attacked when attacker control the jdbc url or properties. pgjdbc instantiates plugin instances based on class names provided via `authenticationPluginClassName`, `sslhostnameverifier`, `socketFactory`, `sslfactory`, `sslpasswordcallback` connection properties. However, the driver did not verify if the class implements the expected interface before instantiating the class. This can lead to code execution loaded via arbitrary classes. Users using plugins are advised to upgrade. There are no known workarounds for this issue.
- CVE-2023-1206: A hash collision flaw was found in the IPv6 connection lookup table in the Linux kernel’s IPv6 functionality when a user makes a new kind of SYN flood attack. A user located in the local network or with a high bandwidth connection can increase the CPU usage of the server that accepts IPV6 connections up to 95%.
- CVE-2023-3338: A null pointer dereference flaw was found in the Linux kernel's DECnet networking protocol. This issue could allow a remote user to crash the system.
- CVE-2023-34319: The fix for XSA-423 added logic to Linux'es netback driver to deal with a frontend splitting a packet in a way such that not all of the headers would come in one piece. Unfortunately the logic introduced there didn't account for the extreme case of the entire packet being split into as many pieces as permitted by the protocol, yet still being smaller than the area that's specially dealt with to keep all (possible) headers together. Such an unusual packet would therefore trigger a buffer overrun in the driver.
- CVE-2023-34324: Closing of an event channel in the Linux kernel can result in a deadlock. This happens when the close is being performed in parallel to an unrelated Xen console action and the handling of a Xen console interrupt in an unprivileged guest.

  The closing of an event channel is e.g. triggered by removal of a paravirtual device on the other side. As this action will cause console messages to be issued on the other side quite often, the chance of triggering the deadlock is not neglectable.

  Note that 32-bit Arm-guests are not affected, as the 32-bit Linux kernel on Arm doesn't use queued-RW-locks, which are required to trigger the issue (on Arm32 a waiting writer doesn't block further readers to get the lock).
- CVE-2023-3863: A use-after-free flaw was found in nfc_llcp_find_local in net/nfc/llcp_core.c in NFC in the Linux kernel. This flaw allows a local user with special privileges to impact a kernel information leak issue.
- CVE-2023-4194: A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - a096ccca6e50 ("tun: tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce ("tap: tap_open(): correctly initialize socket uid"), pass "inode->i_uid" to sock_init_data_uid() as the last parameter and that turns out to not be accurate.
- CVE-2023-3341: The code that processes control channel messages sent to `named` calls certain functions recursively during packet parsing. Recursion depth is only limited by the maximum accepted packet size; depending on the environment, this may cause the packet-parsing code to run out of available stack memory, causing `named` to terminate unexpectedly. Since each incoming control channel message is fully parsed before its contents are authenticated, exploiting this flaw does not require the attacker to hold a valid RNDC key; only network access to the control channel's configured TCP port is necessary.

  This issue affects BIND 9 versions 9.2.0 through 9.16.43, 9.18.0 through 9.18.18, 9.19.0 through 9.19.16, 9.9.3-S1 through 9.16.43-S1, and 9.18.0-S1 through 9.18.18-S1.
- CVE-2021-4001: A race condition was found in the Linux kernel's ebpf verifier between bpf_map_update_elem and bpf_map_freeze due to a missing lock in kernel/bpf/syscall.c. In this flaw, a local user with a special privilege (cap_sys_admin or cap_bpf) can modify the frozen mapped address space. This flaw affects kernel versions prior to 5.16 rc2.

- CVE-2021-46174: Heap-based Buffer Overflow in function bfd_getl32 in Binutils objdump 3.37.
- CVE-2022-35205: An issue was discovered in Binutils readelf 2.38.50, reachable assertion failure in function display_debug_names allows attackers to cause a denial of service.
- CVE-2022-44840: Heap buffer overflow vulnerability in binutils readelf before 2.40 via function find_section_in_set in file readelf.c.
- CVE-2022-45703: Heap buffer overflow vulnerability in binutils readelf before 2.40 via function display_debug_section in file readelf.c.
- CVE-2022-47008: An issue was discovered function make_tempdir, and make_tempname in bucomm.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.
- CVE-2020-19726: An issue was discovered in binutils libbfd.c 2.36 relating to the auxiliary symbol data allows attackers to read or write to system memory or cause a denial of service.
- CVE-2023-51385: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.
- CVE-2023-41040: GitPython is a python library used to interact with Git repositories. In order to resolve some git references, GitPython reads files from the `.git` directory, in some places the name of the file being read is provided by the user, GitPython doesn't check if this file is located outside the `.git` directory. This allows an attacker to make GitPython read any file from the system. This vulnerability is present in https://github.com/gitpython-developers/GitPython/blob/1c8310d7cae144f74a671cbe17e51f63a830adbf/git/refs/symbolic.py#L174-L175. That code joins the base directory with a user given string without checking if the final path is located outside the base directory. This vulnerability cannot be used to read the contents of files but could in theory be used to trigger a denial of service for the program. This issue has not yet been addressed.
- CVE-2023-5178: A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the NVMe/TCP subsystem in the Linux kernel. This issue may allow a malicious user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation.
- CVE-2023-5717: A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation.

  If perf_read_group() is called while an event's sibling_list is smaller than its child's sibling_list, it can increment or write to memory locations outside of the allocated buffer.

  We recommend upgrading past commit 32671e3799ca2e4590773fd0e63aaa4229e50c06.
- CVE-2018-25091: urllib3 before 1.24.2 does not remove the authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or scheme). This can allow for credentials in the authorization header to be exposed to unintended hosts or transmitted in cleartext. Note: his issue exists because of an incomplete fix for CVE-2018-20060 (which was case-sensitive).
- CVE-2023-38552: When the Node.js policy feature checks the integrity of a resource against a trusted manifest, the application can intercept the operation and return a forged checksum to the node's policy implementation, thus effectively disabling the integrity check.
- Impacts: This vulnerability affects all users using the experimental policy mechanism in all active release lines: 18.x and, 20.x. Note that at the time this CVE was issued, the policy mechanism is an experimental feature of Node.js.
- CVE-2019-15847: The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same.
- CVE-2018-13410: An issue was discovered IW44Image.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.
- CVE-2021-46312: An issue was discovered IW44EncodeCodec.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.
- CVE-2021-31239: An issue found in SQLite SQLite3 v.3.35.4 that allows a remote attacker to cause a denial of service via the appendvfs.c function.
- CVE-2021-45346: A Memory Leak vulnerability exists in SQLite Project SQLite3 3.35.1 and 3.37.0 via maliciously crafted SQL Queries (made via editing the Database File), it is possible to query a record, and leak

subsequent bytes of memory that extend beyond the record, which could let a malicious user obtain sensitive information. NOTE: The developer disputes this as a vulnerability stating that If you give SQLite a corrupted database file and submit a query against the database, it might read parts of the database that you did not intend or expect.
- CVE-2023-32570: VideoLAN dav1d before 1.2.0 has a thread_task.c race condition that can lead to an application crash, related to dav1d_decode_frame_exit.
- TEMP-0841856-B18BAF
- CVE-2018-13410: Info-ZIP Zip 3.0, when the -T and -TT command-line options are used, allows attackers to cause a denial of service (invalid free and application crash) or possibly have unspecified other impact because of an off-by-one error. NOTE: it is unclear whether there are realistic scenarios in which an untrusted party controls the -TT value, given that the entire purpose of -TT is execution of arbitrary commands
- CVE-2024-28757: libexpat through 2.6.1 allows an XML Entity Expansion attack when there is isolated use of external parsers (created via XML_ExternalEntityParserCreate).
- CVE-2012-0039: GLib 2.31.8 and earlier, when the g_str_hash function is used, computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table. NOTE: this issue may be disputed by the vendor; the existence of the g_str_hash function is not a vulnerability in the library, because callers of g_hash_table_new and g_hash_table_new_full can specify an arbitrary hash function that is appropriate for the application.
- CVE-2022-2817: Use After Free in GitHub repository vim/vim prior to 9.0.0213.
- CVE-2022-2862: Use After Free in GitHub repository vim/vim prior to 9.0.0221.
- CVE-2022-2874: NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0224.
- CVE-2022-2889: Use After Free in GitHub repository vim/vim prior to 9.0.0225.
- CVE-2022-2982: Use After Free in GitHub repository vim/vim prior to 9.0.0260.
- CVE-2022-3016: Use After Free in GitHub repository vim/vim prior to 9.0.0286.
- CVE-2022-3099: Use After Free in GitHub repository vim/vim prior to 9.0.0360.
- CVE-2022-3134: Use After Free in GitHub repository vim/vim prior to 9.0.0389.
- CVE-2014-8166: The browsing feature in the server in CUPS does not filter ANSI escape sequences from shared printer names, which might allow remote attackers to execute arbitrary code via a crafted printer name.

Cumulative hotfixes

The cumulative hotfixes that have been shipped for Cloudera Private Cloud Data Services 1.5.4-CHF1.

CDP Private Cloud Data Services 1.5.4-CHF1

You must upgrade to CDP Private Cloud Data Services 1.5.4 version before using 1.5.4-CHF1.

The cumulative hotfixes for new features, known issues, and fixed issues for 1.5.4-CHF1.

Whats new in CDP Private Cloud Data Services1.5.4-CHF1

New features introduced in this cumulative hotfix release of CDP Private Cloud Data Services 1.5.4-CHF1.

Note: Cloudera Manager 7.11.3 CHF7 Data Services (version: 7.11.3.14) support CDP Private Cloud Data Services 1.5.4 CHF1 release.

Note: Cloudera Manager 7.11.3 CHF8 does not support any CDP Private Cloud Data Services release.

Restore CP namespaces independently from system-generated DRS backups

Enhancements to the system-generated DRS backups:

- System-generated backups in DRS are automatic, periodic backups that include control plane and data services' namespaces.
- Through Private Cloud Data Services 1.5.4 release, restoring a system-generated backup from the private cloud management console UI restores all the namespaces present in the backup.
- With this change, such a restore action independently restores only control plane namespaces that are present in the backup.

Fixed Issues in CDP Private Cloud Data Services 1.5.4-CHF1

The fixes in this cumulative hotfix release of CDP Private Cloud Data Services 1.5.4-CHF1.

OPSX-5147: OOM when retrieving size of Binary File

Diagnostics bundle collection no longer fails due to OOM errors.

OPSX-5148: Diagnostics Collection from UI w/ Default No Time Limit Should Not Invoke Timestamp Filtering

The diagnostics collection triggered through the UI, with the default "No Time Limit selected", no longer filters logs by timestamp.

Repository Locations for 1.5.4-CHF1

The URLs for CDP Private Cloud Data Services 1.5.4-CHF1 are listed in the following table:

URL Type	Repository Location
Index	`https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4-h2/`
Manifest	Repository: `https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4-h2/manifest.json`
Parcels	Repository: `https://username:password@archive.cloudera.com/p/cdp-pvc-ds/1.5.4-h2/parcels/`

Fixed Common Vulnerabilities and Exposures in 1.5.4 CHF1

Review the Common vulnerabilities and Exposures (CVEs) that were fixed in 1.5.4 CHF1 release of CDP Private Cloud Data Services.

Issue ID	Description
CVE-2004-0230	TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived c
CVE-2005-3660	Linux kernel 2.4 and 2.6 allows attackers to cause a denial of service (memory exhaustion and panic) by creating a socketpairs and setting a large data transfer buffer, then preventing Linux from being able to finish the transfer by c closing the file descriptor without closing an associated reference.
CVE-2007-3719	The process scheduler in the Linux kernel 2.6.16 gives preference to "interactive" processes that perform voluntary denial of service (CPU consumption), as described in "Secretly Monopolizing the CPU Without Superuser Privileg
CVE-2008-2544	Mounting /proc filesystem via chroot command silently mounts it in read-write mode. The user could bypass the ch files, he would never have otherwise.
CVE-2008-4609	The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco produ allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipu demonstrated by sockstress.
CVE-2009-5155	In the GNU C Library (aka glibc or libc6) before 2.28, parse_reg_exp in posix/regcomp.c misparses alternatives, w service (assertion failure and application exit) or trigger an incorrect result by attempting a regular-expression matc

CVE-2010-4563	The Linux kernel, when using IPv6, allows remote attackers to determine whether a host is sniffing the network by multicast address and determining whether an Echo Reply is sent, as demonstrated by thcping.
CVE-2010-5321	Memory leak in drivers/media/video/videobuf-core.c in the videobuf subsystem in the Linux kernel 2.6.x through 4 of service (memory consumption) by leveraging /dev/video access for a series of mmap calls that require new alloc CVE-2007-6761. NOTE: as of 2016-06-18, this affects only 11 drivers that have not been updated to use videobuf2
CVE-2011-4915	fs/proc/base.c in the Linux kernel through 3.1 allows local users to obtain sensitive keystroke information via acces
CVE-2011-4916	Linux kernel through 3.1 allows local users to obtain sensitive keystroke information via access to /dev/pts/ and /de
CVE-2011-4917	In the Linux kernel through 3.1 there is an information disclosure issue via /proc/stat.
CVE-2012-4542	block/scsi_ioctl.c in the Linux kernel through 3.8 does not properly consider the SCSI device class during authoriz users to bypass intended access restrictions via an SG_IO ioctl call that leverages overlapping opcodes.
CVE-2012-6702	Expat, when used in a parser that has not called XML_SetHashSalt or passed it a seed of 0, makes it easier for cont cryptographic protection mechanisms via vectors involving use of the srand function.
CVE-2012-6711	A heap-based buffer overflow exists in GNU Bash before 4.3 when wide characters, not supported by the current lo variable, are printed through the echo built-in function. A local attacker, who can provide data to print through the to crash a script or execute code with the privileges of the bash process. This occurs because ansicstr() in lib/sh/strt
CVE-2013-0341	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was w showed that it was not a security issue. Notes: none.
CVE-2013-1664	The XML libraries for Python 3.4, 3.3, 3.2, 3.1, 2.7, and 2.6, as used in OpenStack Keystone Essex, Folsom, and G Cinder Folsom; Django; and possibly other products allow remote attackers to cause a denial of service (resource c Expansion (XEE) attack.
CVE-2013-1665	The XML libraries for Python 3.4, 3.3, 3.2, 3.1, 2.7, and 2.6, as used in OpenStack Keystone Essex and Folsom, Dj remote attackers to read arbitrary files via an XML external entity declaration in conjunction with an entity referen attack.
CVE-2013-7040	Python 2.7 before 3.4 only uses the last eight bits of the prefix to randomize hash values, which causes it to compu to trigger hash collisions predictably and makes it easier for context-dependent attackers to cause a denial of servic application that maintains a hash table.  **Note:** This vulnerability exists because of an incomplete fix for CVE-2012-1150.
CVE-2014-3477	The dbus-daemon in D-Bus 1.2.x through 1.4.x, 1.6.x before 1.6.20, and 1.8.x before 1.8.4, sends an AccessDenied the client is prohibited from accessing the service, which allows local users to cause a denial of service (initializatio channel attack via a D-Bus message to an inactive service.
CVE-2014-3532	dbus 1.3.0 before 1.6.22 and 1.8.x before 1.8.6, when running on Linux 2.6.37-rc4 or later, allows local users to ca of other services or applications) by sending a message containing a file descriptor, then exceeding the maximum r forwarded.
CVE-2014-3533	dbus 1.3.0 before 1.6.22 and 1.8.x before 1.8.6 allows local users to cause a denial of service (disconnect) via a cer the dbus-daemon to forward a message containing an invalid file descriptor.
CVE-2014-3564	Multiple heap-based buffer overflows in the status_handler function in (1) engine-gpgsm.c and (2) engine-uiserver. attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to "different lin
CVE-2014-3566	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
CVE-2014-3591	Libgcrypt before 1.6.3 and GnuPG before 1.4.19 does not implement ciphertext blinding for Elgamal decryption, w obtain the server's private key by determining factors using crafted ciphertext and the fluctuations in the electromag
CVE-2014-3636	D-Bus 1.3.0 through 1.6.x before 1.6.24 and 1.8.x before 1.8.8 allows local users to (1) cause a denial of service (p drop) by queuing the maximum number of file descriptors or (2) cause a denial of service (disconnect) via multiple allowed number of file descriptors for a single sendmsg call.
CVE-2014-3637	D-Bus 1.3.0 through 1.6.x before 1.6.24 and 1.8.x before 1.8.8 does not properly close connections for processes th to cause a denial of service via a D-bus message containing a D-Bus connection file descriptor.
CVE-2014-3638	The bus_connections_check_reply function in config-parser.c in D-Bus before 1.6.24 and 1.8.x before 1.8.8 allows consumption) via a large number of method calls.
CVE-2014-3639	The dbus-daemon in D-Bus before 1.6.24 and 1.8.x before 1.8.8 does not properly close old connections, which all (incomplete connection consumption and prevention of new connections) via a large number of incomplete connec

CVE-2014-4043	The posix_spawn_file_actions_addopen function in glibc before 2.20 does not copy its path argument in accordanc context-dependent attackers to trigger use-after-free vulnerabilities.
CVE-2014-4617	The do_uncompress function in g10/compress.c in GnuPG 1.x before 1.4.17 and 2.x before 2.0.24 allows context-d service (infinite loop) via malformed compressed packets, as demonstrated by an a3 01 5b ff byte sequence.
CVE-2014-5044	Multiple integer overflows in libgfortran might allow remote attackers to execute arbitrary code or cause a denial o vectors related to array allocation.
CVE-2014-5270	Libgcrypt before 1.5.4, as used in GnuPG and other products, does not properly perform ciphertext normalization a easier for physically proximate attackers to conduct key-extraction attacks by leveraging the ability to collect volta than CVE-2013-4576.
CVE-2014-5351	The kadm5_randkey_principal_3 function in lib/kadm5/srv/svr_principal.c in kadmind in MIT Kerberos 5 (aka krb a -randkey -keepold request, which allows remote authenticated users to forge tickets by leveraging administrative
CVE-2014-5461	Buffer overflow in the vararg functions in ldo.c in Lua 5.1 through 5.2.x before 5.2.3 allows context-dependent atta a small number of arguments to a function with a large number of fixed arguments.
CVE-2014-9114	Blkid in util-linux before 2.26rc-1 allows local users to execute arbitrary code.
CVE-2014-9620	The ELF parser in file 5.08 through 5.21 allows remote attackers to cause a denial of service via a large number of
CVE-2014-9892	The snd_compr_tstamp function in sound/core/compress_offload.c in the Linux kernel through 4.7, as used in And (2013) devices, does not properly initialize a timestamp data structure, which allows attackers to obtain sensitive in Android internal bug 28770164 and Qualcomm internal bug CR568717.
CVE-2014-9900	The ethtool_get_wol function in net/core/ethtool.c in the Linux kernel through 4.7, as used in Android before 2016 not initialize a certain data structure, which allows local users to obtain sensitive information via a crafted applicati Qualcomm internal bug CR570754.
CVE-2014-9939	ihex.c in GNU Binutils before 2.26 contains a stack buffer overflow when printing bad bytes in Intel Hex objects.
CVE-2015-0245	D-Bus 1.4.x through 1.6.x before 1.6.30, 1.8.x before 1.8.16, and 1.9.x before 1.9.10 does not validate the source o local users to cause a denial of service (activation failure error returned) by leveraging a race condition involving s systemd responds.
CVE-2015-0247	Heap-based buffer overflow in openfs.c in the libext2fs library in e2fsprogs before 1.42.12 allows local users to ex descriptor data in a filesystem image.
CVE-2015-0837	The mpi_powm function in Libgcrypt before 1.6.3 and GnuPG before 1.4.19 allows attackers to obtain sensitive in when accessing a pre-computed table during modular exponentiation, related to a "Last-Level Cache Side-Channel
CVE-2015-1197	cpio 2.11, when using the --no-absolute-filenames option, allows local users to write to arbitrary files via a symlink
CVE-2015-1572	Heap-based buffer overflow in closefs.c in the libext2fs library in e2fsprogs before 1.42.12 allows local users to ex block group descriptor to be marked as dirty. NOTE: this vulnerability exists because of an incomplete fix for CVE
CVE-2015-1606	The keyring DB in GnuPG before 2.1.2 does not properly handle invalid packets, which allows remote attackers to use-after-free) via a crafted keyring file.
CVE-2015-1607	kbx/keybox-search.c in GnuPG before 1.4.19, 2.0.x before 2.0.27, and 2.1.x before 2.1.2 does not properly handle attackers to cause a denial of service (invalid read operation) via a crafted keyring file, related to sign extensions ar
CVE-2015-2059	The stringprep_utf8_to_ucs4 function in libin before 1.31, as used in jabberd2, allows context-dependent attackers other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read.
CVE-2015-2327	PCRE before 8.36 mishandles the /(((a\2)|(a*)\g<-1>))*/ pattern and related patterns with certain internal recursive attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted re JavaScript RegExp object encountered by Konqueror.
CVE-2015-2328	PCRE before 8.36 mishandles the /((?(R)a|(?1)))+/ pattern and related patterns with certain recursion, which allows (segmentation fault) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by Konqueror.
CVE-2015-2613	Unspecified vulnerability in Oracle Java SE 7u80 and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote related to JCE.
CVE-2015-2695	lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) before 1.14 relies on an inappropriate context hand denial of service (incorrect pointer read and process crash) via a crafted SPNEGO packet that is mishandled during
CVE-2015-2696	lib/gssapi/krb5/iakerb.c in MIT Kerberos 5 (aka krb5) before 1.14 relies on an inappropriate context handle, which service (incorrect pointer read and process crash) via a crafted IAKERB packet that is mishandled during a gss_inq
CVE-2015-2697	The build_principal_va function in lib/krb5/krb/bld_princ.c in MIT Kerberos 5 (aka krb5) before 1.14 allows remo service (out-of-bounds read and KDC crash) via an initial '\0' character in a long realm field within a TGS request.

CVE-2015-2808	The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key d makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sni on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the
CVE-2015-2877	Kernel Samepage Merging (KSM) in the Linux kernel 2.6.32 through 4.x does not prevent use of a write-timing sid defeat the ASLR protection mechanism on other guest OS instances via a Cross-VM ASL INtrospection (CAIN) at if you care about this attack vector, disable deduplication." Share-until-written approaches for memory conservatio inherently detectable for information disclosure, and can be classified as potentially misunderstood behaviors rathe
CVE-2015-3153	The default configuration for cURL and libcurl before 7.42.1 sends custom HTTP headers to both the proxy and de proxy servers to obtain sensitive information by reading the header contents.
CVE-2015-3217	PCRE 7.8 and 8.32 through 8.37, and PCRE2 10.10 mishandle group empty matches, which might allow remote at based buffer overflow) via a crafted regular expression, as demonstrated by /^(?:(?(1)\\.|([^\\\\W_])?)+)+$/.
CVE-2015-5073	Heap-based buffer overflow in the find_fixedlength function in pcre_compile.c in PCRE before 8.38 allows remote or obtain sensitive information from heap memory and possibly bypass the ASLR protection mechanism via a craft parenthesis.
CVE-2015-5186	Audit before 2.4.4 in Linux does not sanitize escape characters in filenames.
CVE-2015-5218	Buffer overflow in text-utils/colcrt.c in colcrt in util-linux before 2.27 allows local users to cause a denial of service global variable.
CVE-2015-5276	The std::random_device class in libstdc++ in the GNU Compiler Collection (aka GCC) before 4.9.4 does not prope which makes it easier for context-dependent attackers to predict the random values via unspecified vectors.
CVE-2015-7036	The fts3_tokenizer function in SQLite, as used in Apple iOS before 8.4 and OS X before 10.10.4, allows remote att denial of service (application crash) via a SQL command that triggers an API call with a crafted pointer value in th
CVE-2015-8382	The match function in pcre_exec.c in PCRE before 8.37 mishandles the /(?:((abcd))|(((?:(?:(?:(?:abc|(?:abcdef))))b) and related patterns involving (*ACCEPT), which allows remote attackers to obtain sensitive information from pro (partially initialized memory and application crash) via a crafted regular expression, as demonstrated by a JavaScri aka ZDI-CAN-2547.
CVE-2015-8386	PCRE before 8.38 mishandles the interaction of lookbehind assertions and mutually recursive subpatterns, which a service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrate by Konqueror.
CVE-2015-8388	PCRE before 8.38 mishandles the /(?=di(?<=(?1))|(?=(.)))/ pattern and related patterns with an unmatched closing cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expressio object encountered by Konqueror.
CVE-2015-8391	The pcre_compile function in pcre_compile.c in PCRE before 8.38 mishandles certain [: nesting, which allows rem (CPU consumption) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by Konqueror.
CVE-2015-8538	dwarf_leb.c in libdwarf allows attackers to cause a denial of service (SIGSEGV).
CVE-2015-8865	The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34 mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer execute arbitrary code via a crafted magic file.
CVE-2015-8948	idn in GNU libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a z bounds read.
CVE-2015-8982	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-depe (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
CVE-2015-8982	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-depe (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
CVE-2015-8983	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) be to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a buffer overflow.
CVE-2015-8983	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) be to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a buffer overflow.
CVE-2015-8984	The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attacke crash) via a malformed pattern, which triggers an out-of-bounds read.
CVE-2015-8985	The pop_fail_stack function in the GNU C Library (aka glibc or libc6) allows context-dependent attackers to cause application crash) via vectors related to extended regular expression processing.

CVE-2016-0755	The ConnectionExists function in lib/url.c in libcurl before 7.47.0 does not properly re-use NTLM-authenticated pr attackers to authenticate as other users via a request, a similar issue to CVE-2014-0015.
CVE-2016-10228	The iconv program in the GNU C Library (aka glibc or libc6) 2.31 and earlier, when invoked with multiple suffixe or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, l
CVE-2016-10254	The allocate_elf function in common.h in elfutils before 0.168 allows remote attackers to cause a denial of service memory allocation failure.
CVE-2016-10255	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause sh_off or (2) sh_size ELF header value, which triggers a memory allocation failure.
CVE-2016-10255	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause sh_off or (2) sh_size ELF header value, which triggers a memory allocation failure.
CVE-2016-10255	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause sh_off or (2) sh_size ELF header value, which triggers a memory allocation failure.
CVE-2016-10505	NULL pointer dereference vulnerabilities in the imagetopnm function in convert.c, sycc444_to_rgb function in col and sycc422_to_rgb function in color.c in OpenJPEG before 2.2.0 allow remote attackers to cause a denial of servi
CVE-2016-10506	Division-by-zero vulnerabilities in the functions opj_pi_next_cprl, opj_pi_next_pcrl, and opj_pi_next_rpcl in pi.c i attackers to cause a denial of service (application crash) via crafted j2k files.
CVE-2016-10723	An issue was discovered in the Linux kernel through 4.17.2. Since the page allocator does not yield CPU resources unprivileged user can trivially lock up the system forever by wasting CPU resources from the page allocator (e.g., v global OOM killer is invoked. NOTE: the software maintainer has not accepted certain proposed patches, in part be problem is non-trivial to handle.
CVE-2016-1234	Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_A dependent attackers to cause a denial of service (crash) via a long name.
CVE-2016-1938	The s_mp_div function in lib/freebl/mpi/mpi.c in Mozilla Network Security Services (NSS) before 3.21, as used in divides numbers, which might make it easier for remote attackers to defeat cryptographic protection mechanisms b mp_exptmod function.
CVE-2016-1951	Multiple integer overflows in io/prprf.c in Mozilla Netscape Portable Runtime (NSPR) before 4.12 allow remote at overflow) or possibly have unspecified other impact via a long string to a PR_*printf function.
CVE-2016-2037	The cpio_safer_name_suffix function in util.c in cpio 2.11 allows remote attackers to cause a denial of service (out
CVE-2016-2183	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a lon by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
CVE-2016-2226	Integer overflow in the string_appends function in cplus-dem.c in libiberty allows remote attackers to execute arbit triggers a buffer overflow.
CVE-2016-2779	runuser in util-linux allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushe
CVE-2016-3189	Use-after-free vulnerability in bzip2recover in bzip2 1.0.6 allows remote attackers to cause a denial of service (cras ends set to before the start of the block.
CVE-2016-4008	The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.8, when used without the ASN1_ allows remote attackers to cause a denial of service (infinite recursion) via a crafted certificate.
CVE-2016-4429	Stack-based buffer overflow in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or l of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets.
CVE-2016-4472	The overflow protection in Expat is removed by compilers with certain optimization settings, which allows remote or possibly execute arbitrary code via crafted XML data. NOTE: this vulnerability exists because of an incomplete
CVE-2016-4483	The xmlBufAttrSerializeTxtContent function in xmlsave.c in libxml2 allows context-dependent attackers to cause a application crash) via a non-UTF-8 attribute value, related to serialization. NOTE: this vulnerability may be a dupli
CVE-2016-4484	The Debian initrd script for the cryptsetup package 2:1.7.3-2 and earlier allows physically proximate attackers to g an invalid password.
CVE-2016-4487	Use-after-free vulnerability in libiberty allows remote attackers to cause a denial of service (segmentation fault and "btypevec."
CVE-2016-4488	Use-after-free vulnerability in libiberty allows remote attackers to cause a denial of service (segmentation fault and "ktypevec."
CVE-2016-4489	Integer overflow in the gnu_special function in libiberty allows remote attackers to cause a denial of service (segm related to the "demangling of virtual tables."

CVE-2016-4490	Integer overflow in cp-demangle.c in libiberty allows remote attackers to cause a denial of service (segmentation fa inconsistent use of the long and int types for lengths.
CVE-2016-4491	The d_print_comp function in cp-demangle.c in libiberty allows remote attackers to cause a denial of service (segm which triggers infinite recursion and a buffer overflow, related to a node having "itself as ancestor more than once."
CVE-2016-4492	Buffer overflow in the do_type function in cplus-dem.c in libiberty allows remote attackers to cause a denial of ser crafted binary.
CVE-2016-4493	The demangle_template_value_parm and do_hpacc_template_literal functions in cplus-dem.c in libiberty allow rer (out-of-bounds read and crash) via a crafted binary.
CVE-2016-4984	/usr/libexec/openldap/generate-server-cert.sh in openldap-servers sets weak permissions for the TLS certificate, wh certificate by leveraging a race condition between the creation of the certificate, and the chmod to protect it.
CVE-2016-5300	The XML parser in Expat does not use sufficient entropy for hash initialization, which allows context-dependent at consumption) via crafted identifiers in an XML document. NOTE: this vulnerability exists because of an incomplet
CVE-2016-6153	os_unix.c in SQLite before 3.13.0 improperly implements the temporary directory search algorithm, which might a information, cause a denial of service (application crash), or have unspecified other impact by leveraging use of the files.
CVE-2016-6261	The idna_to_ascii_4i function in lib/idna.c in libidn before 1.33 allows context-dependent attackers to cause a deni via 64 bytes of input.
CVE-2016-6262	idn in libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero by read, a different vulnerability than CVE-2015-8948.
CVE-2016-6263	The stringprep_utf8_nfkc_normalize function in lib/nfkc.c in libidn before 1.33 allows context-dependent attackers read and crash) via crafted UTF-8 data.
CVE-2016-6318	Stack-based buffer overflow in the FascistGecosUser function in lib/fascist.c in cracklib allows local users to cause privileges via a long GECOS field, involving longbuffer.
CVE-2016-6321	Directory traversal vulnerability in the safer_name_suffix function in GNU tar 1.14 through 1.29 might allow remo mechanism and write to arbitrary files via vectors related to improper sanitization of the file_name parameter, aka
CVE-2016-6349	The machinectl command in oci-register-machine allows local users to list running containers and possibly obtain s command.
CVE-2016-7091	sudo: It was discovered that the default sudo configuration on Red Hat Enterprise Linux and possibly other Linux i INPUTRC which could lead to information disclosure. A local user with sudo access to a restricted program that us from specially formatted files with elevated privileges provided by sudo.
CVE-2016-8615	A flaw was found in curl before version 7.51. If cookie state is written into a cookie jar file that is later read back a HTTP server can inject new cookies for arbitrary domains into said cookie jar.
CVE-2016-8616	A flaw was found in curl before version 7.51.0 When re-using a connection, curl was doing case insensitive compa existing connections. This means that if an unused connection with proper credentials exists for a protocol that has can cause that connection to be reused if s/he knows the case-insensitive version of the correct password.
CVE-2016-8617	The base64 encode function in curl before version 7.51.0 is prone to a buffer being under allocated in 32bit system `CURLOPT_USERNAME`.
CVE-2016-8618	The libcurl API function called `curl_maprintf()` before version 7.51.0 can be tricked into doing a double-free due systems using 32 bit `size_t` variables.
CVE-2016-8619	The function `read_data()` in security.c in curl before version 7.51.0 is vulnerable to memory double free.
CVE-2016-8621	The `curl_getdate` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an inpu
CVE-2016-8622	The URL percent-encoding decode function in libcurl before 7.51.0 is called `curl_easy_unescape`. Internally, ever unscape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.
CVE-2016-8623	A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use
CVE-2016-8624	curl before version 7.51.0 doesn't parse the authority component of the URL correctly when the host name part end tricked into connecting to a different host. This may have security implications if you for example use an URL pars domains before using curl to request them.
CVE-2016-8625	curl before version 7.51.0 uses outdated IDNA 2003 standard to handle International Domain Names and this may issue network transfer requests to the wrong host.
CVE-2016-9063	An integer overflow during the parsing of XML using the Expat library. This vulnerability affects Firefox < 50.

CVE-2016-9074	An existing mitigation of timing side-channel attacks is insufficient in some circumstances. This issue is addressed This vulnerability affects Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.
CVE-2016-9113	There is a NULL pointer dereference in function imagetobmp of convertbmp.c:980 of OpenJPEG 2.1.2. image->co initialization(NULL). Impact is Denial of Service.
CVE-2016-9114	There is a NULL Pointer Access in function imagetopnm of convert.c:1943(jp2) of OpenJPEG 2.1.2. image->comp initialization(NULL). Impact is Denial of Service.
CVE-2016-9115	Heap Buffer Over-read in function imagetotga of convert.c(jp2):942 in OpenJPEG 2.1.2. Impact is Denial of Servi
CVE-2016-9116	NULL Pointer Access in function imagetopnm of convert.c:2226(jp2) in OpenJPEG 2.1.2. Impact is Denial of Serv
CVE-2016-9117	NULL Pointer Access in function imagetopnm of convert.c(jp2):1289 in OpenJPEG 2.1.2. Impact is Denial of Serv
CVE-2016-9318	libxml2 2.9.4 and earlier, as used in XMLSec 1.2.23 and earlier and other products, does not offer a flag directly in read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity
CVE-2016-9574	nss before version 3.30 is vulnerable to a remote denial of service during the session handshake when using Sessio
CVE-2016-9580	An integer overflow vulnerability was found in tiftoimage function in openjpeg 2.1.2, resulting in heap buffer over
CVE-2016-9581	An infinite loop vulnerability in tiftoimage that results in heap buffer overflow in convert_32s_C1P1 was found in
CVE-2016-9586	curl before version 7.52.0 is vulnerable to a buffer overflow when doing a large floating point output in libcurl's im are any application that accepts a format string from the outside without necessary input filtering, it could allow rer
CVE-2017-0630	An information disclosure vulnerability in the kernel trace subsystem could enable a local malicious application to This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Vers A-34277115.
CVE-2017-0663	A remote code execution vulnerability in libxml2 could enable an attacker using a specially crafted file to execute a unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application th Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37104170.
CVE-2017-1000100	When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length. This too larg making curl attempt to send more data than what is actually put into the buffer. The endto() function will then read A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client ha redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protoco CURLOPT_REDIR_PROTOCOLS.
CVE-2017-1000158	CPython (aka Python) up to 2.7.13 is vulnerable to an integer overflow in the PyString_DecodeEscape function in overflow (and possible arbitrary code execution)
CVE-2017-1000254	libcurl may read outside of a heap allocated buffer when doing FTP. When libcurl connects to an FTP server and su asks the server for the current directory with the `PWD` command. The server then responds with a 257 response c The returned path name is then kept by libcurl for subsequent uses. Due to a flaw in the string parser for this direct but without a closing double quote would lead to libcurl not adding a trailing NUL byte to the buffer holding the na the string, it could read beyond the allocated heap buffer and crash or wrongly access data beyond the buffer, think server could abuse this fact and effectively prevent libcurl-based clients to work with it - the PWD command is alw mistake has a high chance of causing a segfault. The simple fact that this has issue remained undiscovered for this l responses are rare in benign servers. We are not aware of any exploit of this flaw. This bug was introduced in comm commit/415d2e7cb7), March 2005. In libcurl version 7.56.0, the parser always zero terminates the string but also re double quote.
CVE-2017-10140	Postfix before 2.11.10, 3.0.x before 3.0.10, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 might allow local users to gai functionality in Berkeley DB 2.x and later, related to reading settings from DB_CONFIG in the current directory.
CVE-2017-10684	In ncurses 6.0, there is a stack-based buffer overflow in the fmt_entry function. A crafted input will lead to a remot
CVE-2017-10685	In ncurses 6.0, there is a format string vulnerability in the fmt_entry function. A crafted input will lead to a remote
CVE-2017-10790	The _asn1_check_identifier function in GNU Libtasn1 through 4.12 causes a NULL pointer dereference and crash assignment of a NULL value within an asn1_node structure. It may lead to a remote denial of service attack.
CVE-2017-10989	The getNodeSize function in ext/rtree/rtree.c in SQLite through 3.19.3, as used in GDAL and other products, misha database, leading to a heap-based buffer over-read or possibly unspecified other impact.
CVE-2017-11112	In ncurses 6.0, there is an attempted 0xffffffffffffffff access in the append_acs function of tinfo/parse_entry.c. It co the terminfo library code is used to process untrusted terminfo data.
CVE-2017-11113	In ncurses 6.0, there is a NULL Pointer Dereference in the _nc_parse_entry function of tinfo/parse_entry.c. It could the terminfo library code is used to process untrusted terminfo data.

CVE-2017-11462	Double free vulnerability in MIT Kerberos 5 (aka krb5) allows attackers to have unspecified impact via vectors inv on error.
CVE-2017-12449	The _bfd_vms_save_sized_string function in vms-misc.c in the Binary File Descriptor (BFD) library (aka libbfd), a earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms file.
CVE-2017-12451	The _bfd_xcoff_read_ar_hdr function in bfd/coff-rs6000.c and bfd/coff64-rs6000.c in the Binary File Descriptor (B GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds stack read via a crafted COFF im
CVE-2017-12452	The bfd_mach_o_i386_canonicalize_one_reloc function in bfd/mach-o-i386.c in the Binary File Descriptor (BFD) Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted mach-o file.
CVE-2017-12453	The _bfd_vms_slurp_eeom function in libbfd.c in the Binary File Descriptor (BFD) library (aka libbfd), as distribu remote attackers to cause an out of bounds heap read via a crafted vms alpha file.
CVE-2017-12454	The _bfd_vms_slurp_egsd function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as allows remote attackers to cause an arbitrary memory read via a crafted vms alpha file.
CVE-2017-12455	The evax_bfd_print_emh function in vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distri allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.
CVE-2017-12456	The read_symbol_stabs_debugging_info function in rddbg.c in GNU Binutils 2.29 and earlier allows remote attack crafted binary file.
CVE-2017-12457	The bfd_make_section_with_flags function in section.c in the Binary File Descriptor (BFD) library (aka libbfd), as allows remote attackers to cause a NULL dereference via a crafted file.
CVE-2017-12458	The nlm_swap_auxiliary_headers_in function in bfd/nlmcode.h in the Binary File Descriptor (BFD) library (aka lib earlier, allows remote attackers to cause an out of bounds heap read via a crafted nlm file.
CVE-2017-12799	The elf_read_notesfunction in bfd/elf.c in GNU Binutils 2.29 allows remote attackers to cause a denial of service (possibly have unspecified other impact via a crafted binary file.
CVE-2017-12967	The getsym function in tekhex.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Bi denial of service (stack-based buffer over-read and application crash) via a malformed tekhex binary.
CVE-2017-13685	The dump_callback function in SQLite 3.20.0 allows remote attackers to cause a denial of service (EXC_BAD_AC file.
CVE-2017-13694	The acpi_ps_complete_final_op() function in drivers/acpi/acpica/psobject.c in the Linux kernel through 4.12.9 doe causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypa kernel through 4.9) via a crafted ACPI table.
CVE-2017-13710	The setup_group function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU B a denial of service (NULL pointer dereference and application crash) via a group section that is too small.
CVE-2017-13728	There is an infinite loop in the next_char function in comp_scan.c in ncurses 6.0, related to libtic. A crafted input w
CVE-2017-13729	There is an illegal address access in the _nc_save_str function in alloc_entry.c in ncurses 6.0. It will lead to a remo
CVE-2017-13730	There is an illegal address access in the function _nc_read_entry_source() in progs/tic.c in ncurses 6.0 that might le
CVE-2017-13731	There is an illegal address access in the function postprocess_termcap() in parse_entry.c in ncurses 6.0 that will lea
CVE-2017-13732	There is an illegal address access in the function dump_uses() in progs/dump_entry.c in ncurses 6.0 that might lead
CVE-2017-13733	There is an illegal address access in the fmt_entry function in progs/dump_entry.c in ncurses 6.0 that might lead to
CVE-2017-13734	There is an illegal address access in the _nc_safe_strcat function in strings.c in ncurses 6.0 that will lead to a remot
CVE-2017-13757	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not validate the Pl attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, rel elf32-i386.c and elf_x86_64_get_synthetic_symtab in elf64-x86-64.c.
CVE-2017-14062	Integer overflow in the decode_digit function in puny_decode.c in Libidn2 before 2.0.4 allows remote attackers to unspecified other impact.
CVE-2017-14128	The decode_line_info function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed i to cause a denial of service (read_1_byte heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-14129	The read_section function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GN cause a denial of service (parse_comp_unit heap-based buffer over-read and application crash) via a crafted ELF fi
CVE-2017-14130	The _bfd_elf_parse_attributes function in elf-attrs.c in the Binary File Descriptor (BFD) library (aka libbfd), as dis attackers to cause a denial of service (_bfd_elf_attr_strdup heap-based buffer over-read and application crash) via a

CVE-2017-14529	The pe_print_idata function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed i vector entries, which allows remote attackers to cause a denial of service (heap-based buffer over-read and applicat bfd_getl16 function.
CVE-2017-14729	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in Gl entry for a symbol, which allows remote attackers to cause a denial of service (heap-based buffer overflow and app other impact via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.
CVE-2017-14745	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in Gl a sorting count instead of an error flag, which allows remote attackers to cause a denial of service (integer overflow unspecified other impact via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.
CVE-2017-14930	Memory leak in decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distribute attackers to cause a denial of service (memory consumption) via a crafted ELF file.
CVE-2017-14932	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binut denial of service (infinite loop) via a crafted ELF file.
CVE-2017-14933	read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU cause a denial of service (infinite loop) via a crafted ELF file.
CVE-2017-14934	process_debug_info in dwarf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binu denial of service (infinite loop) via a crafted ELF file that contains a negative size value in a CU structure.
CVE-2017-14938	_bfd_elf_slurp_version_tables in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GN cause a denial of service (excessive memory allocation and application crash) via a crafted ELF file.
CVE-2017-14939	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binut which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a
CVE-2017-14940	scan_unit_for_symbols in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file.
CVE-2017-14974	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in Gl certain canonicalization step, which allows remote attackers to cause a denial of service (NULL pointer dereferenc related to elf32-i386.c and elf64-x86-64.c.
CVE-2017-15020	dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file, rela demonstrated by a parse_die heap-based buffer over-read.
CVE-2017-15021	bfd_get_debug_link_info_1 in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in G cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to bfd_g
CVE-2017-15022	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not val allows remote attackers to cause a denial of service (bfd_hash_hash NULL pointer dereference, or out-of-bounds a ELF file, related to scan_unit_for_symbols and parse_comp_unit.
CVE-2017-15023	read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU format count, which allows remote attackers to cause a denial of service (NULL pointer dereference and applicatio concat_filename.
CVE-2017-15024	find_abstract_instance_name in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in to cause a denial of service (infinite recursion and application crash) via a crafted ELF file.
CVE-2017-15025	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binut denial of service (divide-by-zero error and application crash) via a crafted ELF file.
CVE-2017-15088	plugins/preauth/pkinit/pkinit_crypto_openssl.c in MIT Kerberos 5 (aka krb5) through 1.15.2 mishandles Distinguis attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) in situations get_matching_data and X509_NAME_oneline_ex functions. NOTE: this has security relevance only in use cases o the use of get_matching_data in KDC certauth plugin code that is specific to Red Hat.
CVE-2017-15225	_bfd_dwarf2_cleanup_debug_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distribut attackers to cause a denial of service (memory leak) via a crafted ELF file.
CVE-2017-15286	SQLite 3.20.1 has a NULL pointer dereference in tableColumnList in shell.c because it fails to consider certain cas `sqlite3_step(pStmt)==SQLITE_ROW` is false and a data structure is never initialized.
CVE-2017-15671	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27, when invoked with GLOB_TIL when processing the ~ operator with a long user name, potentially leading to a denial of service (memory leak).
CVE-2017-15938	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, miscalculate of a relocatable object file, which allows remote attackers to cause a denial of service (find_abstract_instance_nam and application crash).

CVE-2017-15939	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted  **Note:** This issue is caused by an incomplete fix for CVE-2017-15023.
CVE-2017-15996	elfcomm.c in readelf in GNU Binutils 2.29 allows remote attackers to cause a denial of service (excessive memory impact via a crafted ELF file that triggers a "buffer overflow on fuzzed archive header," related to an uninitialized the get_archive_member_name, process_archive_index_and_symbols, and setup_archive functions.
CVE-2017-16826	The coff_slurp_line_table function in coffcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distrib attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified ot
CVE-2017-16827	The aout_get_external_symbols function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as dist remote attackers to cause a denial of service (slurp_symtab invalid free and application crash) or possibly have uns
CVE-2017-16828	The display_debug_frames function in dwarf.c in GNU Binutils 2.29.1 allows remote attackers to cause a denial of buffer over-read, and application crash) or possibly have unspecified other impact via a crafted ELF file, related to
CVE-2017-16829	The _bfd_elf_parse_gnu_properties function in elf-properties.c in the Binary File Descriptor (BFD) library (aka lib does not prevent negative pointers, which allows remote attackers to cause a denial of service (out-of-bounds read unspecified other impact via a crafted ELF file.
CVE-2017-16830	The print_gnu_property_note function in readelf.c in GNU Binutils 2.29.1 does not have integer-overflow protecti attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified ot
CVE-2017-16831	coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not remote attackers to cause a denial of service (integer overflow and application crash, or excessive memory allocati via a crafted PE file.
CVE-2017-16832	The pe_bfd_read_buildid function in peicode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distribu size and offset values in the data dictionary, which allows remote attackers to cause a denial of service (segmentati have unspecified other impact via a crafted PE file.
CVE-2017-16879	Stack-based buffer overflow in the _nc_write_entry function in tinfo/write_entry.c in ncurses 6.0 allows attackers t or possibly execute arbitrary code via a crafted terminfo file, as demonstrated by tic.
CVE-2017-16931	parser.c in libxml2 before 2.9.5 mishandles parameter-entity references because the NEXTL macro calls the xmlPa of a '%' character in a DTD name.
CVE-2017-16932	parser.c in libxml2 before 2.9.5 does not prevent infinite recursion in parameter entities.
CVE-2017-17080	elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not valida allows remote attackers to cause a denial of service (bfd_getl32 heap-based buffer over-read and application crash) elfcore_grok_netbsd_procinfo, elfcore_grok_openbsd_procinfo, and elfcore_grok_nto_status.
CVE-2017-17121	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attacke access violation) or possibly have unspecified other impact via a COFF binary in which a relocation refers to a loca section.
CVE-2017-17122	The dump_relocs_in_section function in objdump.c in GNU Binutils 2.29.1 does not check for reloc count integer cause a denial of service (excessive memory allocation, or heap-based buffer overflow and application crash) or po crafted PE file.
CVE-2017-17123	The coff_slurp_reloc_table function in coffcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distri attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted COFF based f
CVE-2017-17124	The _bfd_coff_read_string_table function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as properly validate the size of the external string table, which allows remote attackers to cause a denial of service (ex buffer overflow and application crash) or possibly have unspecified other impact via a crafted COFF binary.
CVE-2017-17125	nm.c and objdump.c in GNU Binutils 2.29.1 mishandle certain global symbols, which allows remote attackers to ca (_bfd_elf_get_symbol_version_string buffer over-read and application crash) or possibly have unspecified other im
CVE-2017-17126	The load_debug_section function in readelf.c in GNU Binutils 2.29.1 allows remote attackers to cause a denial of s application crash) or possibly have unspecified other impact via an ELF file that lacks section headers.
CVE-2017-17479	In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the pgxtoimage function in jpwl/convert.c. Th write, which may lead to remote denial of service or possibly remote code execution.
CVE-2017-18078	systemd-tmpfiles in systemd before 237 attempts to support ownership/permission changes on hardlinked files ever turned off, which allows local users to bypass intended access restrictions via vectors involving a hard link to a file demonstrated by changing the ownership of the /etc/passwd file.

CVE-2017-18640	The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CV
CVE-2017-5969	libxml2 2.9.4, when used in recover mode, allows remote attackers to cause a denial of service (NULL pointer dere NOTE: The maintainer states "I would disagree of a CVE with the Recover parsing option which should only be us parser.
CVE-2017-6004	The compile_bracket_matchingpath function in pcre_jit_compile.c in PCRE through 8.x before revision 1680 (e.g. remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted regular expres
CVE-2017-6891	Two errors in the "asn1_find_node()" function (lib/parser_aux.c) within GnuTLS libtasn1 version 4.10 can be expl overflow by tricking a user into processing a specially crafted assignments file via the e.g. asn1Coding utility.
CVE-2017-6965	readelf in GNU Binutils 2.28 writes to illegal addresses while processing corrupt input files containing symbol-diff buffer overflow.
CVE-2017-6966	readelf in GNU Binutils 2.28 has a use-after-free (specifically read-after-free) error while processing multiple, relo caused by mishandling of an invalid symbol index, and mishandling of state across invocations.
CVE-2017-6969	readelf in GNU Binutils 2.28 is vulnerable to a heap-based buffer over-read while processing corrupt RL78 binarie crashes. It may lead to an information leak as well.
CVE-2017-7000	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and applicatio
CVE-2017-7186	libpcre1 in PCRE 8.40 and libpcre2 in PCRE2 10.23 allow remote attackers to cause a denial of service (segmentat crash) by triggering an invalid Unicode property lookup.
CVE-2017-7209	The dump_section_as_bytes function in readelf in GNU Binutils 2.28 accesses a NULL pointer while reading secti program crash.
CVE-2017-7210	objdump in GNU Binutils 2.28 is vulnerable to multiple heap-based buffer over-reads (of size 1 and size 8) while h a crafted object file, leading to program crash.
CVE-2017-7223	GNU assembler in GNU Binutils 2.28 is vulnerable to a global buffer overflow (of size 1) while attempting to unge potentially leading to a program crash.
CVE-2017-7224	The find_nearest_line function in objdump in GNU Binutils 2.28 is vulnerable to an invalid write (of size 1) while an empty function name, leading to a program crash.
CVE-2017-7225	The find_nearest_line function in addr2line in GNU Binutils 2.28 does not handle the case where the main file nam triggering a NULL pointer dereference and an invalid write, and leading to a program crash.
CVE-2017-7226	The pe_ILF_object_p function in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binu over-read of size 4049 because it uses the strlen function instead of strnlen, leading to program crashes in several u could lead to information disclosure as well.
CVE-2017-7227	GNU linker (ld) in GNU Binutils 2.28 is vulnerable to a heap-based buffer overflow while processing a bogus inpu relates to lack of '\0' termination of a name field in ldlex.l.
CVE-2017-7244	The _pcre32_xclass function in pcre_xclass.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial o file.
CVE-2017-7299	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an invalid read (of (bfd_elf_final_link function in bfd/elflink.c) does not check the format of the input file before trying to read the EL leads to a GNU linker (ld) program crash.
CVE-2017-7300	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an aout_link_add_s vulnerable to a heap-based buffer over-read (off-by-one) because of an incomplete check for invalid string offsets v linker (ld) program crash.
CVE-2017-7301	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an aout_link_add_s off-by-one vulnerability because it does not carefully check the string offset. The vulnerability could lead to a GNU
CVE-2017-7302	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a swap_std_reloc_o to an invalid read (of size 4) because of missing checks for relocs that could not be recognised. This vulnerability c
CVE-2017-7303	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an inva check (in the find_link function) for null headers before attempting to match them. This vulnerability causes Binuti
CVE-2017-7304	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an inva check (in the copy_special_section_fields function) for an invalid sh_link field before attempting to follow it. This to crash.
CVE-2017-7375	A flaw in libxml2 allows remote XML entity inclusion with default parser flags (i.e., when the caller did not reques DTD subset loading, or default DTD attributes). Depending on the context, this may expose a higher-risk attack su default parser flags, and expose content from local files, HTTP, or FTP servers (which might be otherwise unreach

CVE-2017-7407	The ourWriteOut function in tool_writeout.c in curl 7.53.1 might allow physically proximate attackers to obtain sen opportunistic circumstances by reading a workstation screen during use of a --write-out argument ending in a '%' cl over-read.
CVE-2017-7500	It was found that rpm did not properly handle RPM installations when a destination path was a symbolic link to a d and permissions of an arbitrary directory, and RPM files being placed in an arbitrary destination. An attacker, with subdirectory will be installed, could redirect that directory to an arbitrary location and gain root privilege.
CVE-2017-7501	It was found that versions of rpm before 4.13.0.2 use temporary files with predictable names when installing an RP directory where files will be installed could create symbolic links to an arbitrary location and modify content, and p could be used for denial of service or possibly privilege escalation.
CVE-2017-7526	libgcrypt before version 1.7.8 is vulnerable to a cache side-channel attack resulting into a complete break of RSA-1 computing the sliding-window expansion. The same attack is believed to work on RSA-2048 with moderately mor attacker can run arbitrary software on the hardware where the private RSA key is used.
CVE-2017-7607	The handle_gnu_hash function in readelf.c in elfutils 0.168 allows remote attackers to cause a denial of service (he crash) via a crafted ELF file.
CVE-2017-7608	The ebl_object_note_type_name function in eblobjnotetypename.c in elfutils 0.168 allows remote attackers to caus read and application crash) via a crafted ELF file.
CVE-2017-7609	elf_compress.c in elfutils 0.168 does not validate the zlib compression factor, which allows remote attackers to cau via a crafted ELF file.
CVE-2017-7610	The check_group function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-ba via a crafted ELF file.
CVE-2017-7611	The check_symtab_shndx function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service crash) via a crafted ELF file.
CVE-2017-7612	The check_sysv_hash function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (hea crash) via a crafted ELF file.
CVE-2017-7613	elflint.c in elfutils 0.168 does not validate the number of sections and the number of segments, which allows remot (memory consumption) via a crafted ELF file.
CVE-2017-7614	elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a "memb behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have {return 0;}" program.
CVE-2017-7781	An error occurs in the elliptic curve point addition algorithm that uses mixed Jacobian-affine coordinates where it c when it should not. A man-in-the-middle attacker could use this to interfere with a connection, resulting in an attac secret. This vulnerability affects Firefox < 55.
CVE-2017-7781	An error occurs in the elliptic curve point addition algorithm that uses mixed Jacobian-affine coordinates where it c when it should not. A man-in-the-middle attacker could use this to interfere with a connection, resulting in an attac secret. This vulnerability affects Firefox < 55.
CVE-2017-8392	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an inva to determine whether symbols are NULL in the _bfd_dwarf2_find_nearest_line function. This vulnerability causes programs using the libbfd library, such as objdump, to crash.
CVE-2017-8393	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to a globa assumption made by code that runs for objcopy and strip, that SHT_REL/SHR_RELA sections are always named s vulnerability causes programs that conduct an analysis of binary programs using the libbfd library, such as objcopy
CVE-2017-8394	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an inva dereferencing of _bfd_elf_large_com_section. This vulnerability causes programs that conduct an analysis of binar objcopy, to crash.
CVE-2017-8395	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an inva malloc() return-value check to see if memory had actually been allocated in the _bfd_generic_get_section_contents that conduct an analysis of binary programs using the libbfd library, such as objcopy, to crash.
CVE-2017-8396	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an inva offset range tests didn't catch small negative offsets less than the size of the reloc field. This vulnerability causes pr programs using the libbfd library, such as objdump, to crash.
CVE-2017-8397	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an inva size 1 during processing of a corrupt binary containing reloc(s) with negative addresses. This vulnerability causes p programs using the libbfd library, such as objdump, to crash.
CVE-2017-8398	dwarf.c in GNU Binutils 2.28 is vulnerable to an invalid read of size 1 during dumping of debug information from programs that conduct an analysis of binary programs, such as objdump and readelf, to crash.

CVE-2017-8421	The function coff_set_alignment_hook in coffcode.h in Binary File Descriptor (BFD) library (aka libbfd), as distrib leak vulnerability which can cause memory exhaustion in objdump via a crafted PE file. Additional validation in du resolve this.
CVE-2017-8804	The xdr_bytes and xdr_string functions in the GNU C Library (aka glibc or libc6) 2.25 mishandle failures of buffer attackers to cause a denial of service (virtual memory allocation, or memory consumption if an overcommit setting 111, a related issue to CVE-2017-8779. NOTE: [Information provided from upstream and references
CVE-2017-8817	The FTP wildcard function in curl and libcurl before 7.57.0 allows remote attackers to cause a denial of service (ou possibly have unspecified other impact via a string that ends with an '[' character.
CVE-2017-8872	The htmlParseTryOrFinish function in HTMLparser.c in libxml2 2.9.4 allows attackers to cause a denial of service
CVE-2017-9038	GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and applicatio byte_get_little_endian function in elfcomm.c, the get_unwind_section_word function in readelf.c, and ARM unwin offsets.
CVE-2017-9039	GNU Binutils 2.28 allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF fi get_program_headers function in readelf.c.
CVE-2017-9040	GNU Binutils 2017-04-03 allows remote attackers to cause a denial of service (NULL pointer dereference and appl process_mips_specific function in readelf.c, via a crafted ELF file that triggers a large memory-allocation attempt.
CVE-2017-9041	GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and applicatio MIPS GOT mishandling in the process_mips_specific function in readelf.c.
CVE-2017-9042	readelf.c in GNU Binutils 2017-04-12 has a "cannot be represented in type long" issue, which might allow remote a (application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-9043	readelf.c in GNU Binutils 2017-04-12 has a "shift exponent too large for type unsigned long" issue, which might al service (application crash) or possibly have unspecified other impact via a crafted ELF file.
CVE-2017-9044	The print_symbol_for_build_attribute function in readelf.c in GNU Binutils 2017-04-12 allows remote attackers to SEGV) via a crafted ELF file.
CVE-2017-9047	A buffer overflow was discovered in libxml2 20904-GITv2.9.4-16-g0741801. The function xmlSnprintfElementCo recursively dump the element content definition into a char buffer 'buf' of size 'size'. The variable len is assigned st XML_ELEMENT_CONTENT_ELEMENT, then (i) the content->prefix is appended to buf (if it actually fits) whe buffer. However, the check for whether the content->name actually fits also uses 'len' rather than the updated buffe about "size" many bytes beyond the allocated memory. This vulnerability causes programs that use libxml2, such a
CVE-2017-9048	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a stack-based buffer overflow. The function xmlSnprintfE recursively dump the element content definition into a char buffer 'buf' of size 'size'. At the end of the routine, the f without checking whether the current strlen(buf) + 2 < size. This vulnerability causes programs that use libxml2, su
CVE-2017-9049	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictComputeFast causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for
CVE-2017-9050	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictAddString fu programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for CVE-2
CVE-2017-9233	XML External Entity vulnerability in libexpat 2.2.0 and earlier (Expat XML Parser Library) allows attackers to put malformed external entity definition from an external DTD.
CVE-2017-9742	The score_opcodes function in opcodes/score7-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denia crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this fi
CVE-2017-9743	The print_insn_score32 function in opcodes/score7-dis.c:552 in GNU Binutils 2.28 allows remote attackers to caus and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by misha execution.
CVE-2017-9744	The sh_elf_set_mach_from_flags function in bfd/elf32-sh.c in the Binary File Descriptor (BFD) library (aka libbfd remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified o demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9745	The _bfd_vms_slurp_etir function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as d remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified o demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9746	The disassemble_bytes function in objdump.c in GNU Binutils 2.28 allows remote attackers to cause a denial of se or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of rae insns pri execution.

CVE-2017-9747	The ieee_archive_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other imp by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug.
CVE-2017-9748	The ieee_object_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other imp by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug.
CVE-2017-9749	The *regs* macros in opcodes/bfin-dis.c in GNU Binutils 2.28 allow remote attackers to cause a denial of service (possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during
CVE-2017-9750	opcodes/rx-decode.opc in GNU Binutils 2.28 lacks bounds checks for certain scale arrays, which allows remote att overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated -D" execution.
CVE-2017-9751	opcodes/rl78-decode.opc in GNU Binutils 2.28 has an unbounded GETBYTE macro, which allows remote attacker and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by misha execution.
CVE-2017-9752	bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allov service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, a the _bfd_vms_get_value and _bfd_vms_slurp_etir functions during "objdump -D" execution.
CVE-2017-9753	The versados_mkobject function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distr initialize a certain data structure, which allows remote attackers to cause a denial of service (buffer overflow and ap other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9754	The process_otr function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed i certain offset, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.
CVE-2017-9755	opcodes/i386-dis.c in GNU Binutils 2.28 does not consider the number of registers for bnd mode, which allows rem (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demo "objdump -D" execution.
CVE-2017-9756	The aarch64_ext_ldst_reglist function in opcodes/aarch64-dis.c in GNU Binutils 2.28 allows remote attackers to ca and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by misha execution.
CVE-2017-9954	The getvalue function in tekhex.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU B a denial of service (stack-based buffer over-read and application crash) via a crafted tekhex file, as demonstrated by
CVE-2017-9955	The get_build_id function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GN cause a denial of service (heap-based buffer over-read and application crash) via a crafted file in which a certain siz field, as demonstrated by mishandling within the objdump program.
CVE-2018-1000030	Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions prior to that Python 2.7.17 and prior may also be vulnerable however this has not been confirmed. The vulnerability lies wh amounts of data. In both cases there is essentially a race condition that occurs. For the Heap-Buffer-Overflow, Thre Thread1 is already writing to the buffer without knowing how much to write. So when a large amount of data is bei corruption using a Heap-Buffer-Overflow. As for the Use-After-Free, Thread3->Malloc->Thread1->Free's->Thread stated that this is not a security vulnerability due to the fact that the attacker must be able to run code, however in s this vulnerability can potentially be used by an attacker to violate a trust boundary, as such the DWF feels this issue
CVE-2018-1058	A flaw was found in the way Postgresql allowed a user to modify the behavior of a query for other users. An attack execute code with the permissions of superuser in the database. Versions 9.3 through 10 are affected.
CVE-2018-10754	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was w showed that it was not a security issue.  **Note:** None.
CVE-2018-11212	An issue was discovered in libjpeg 9a and 9d. The alloc_sarray function in jmemmgr.c allows remote attackers to c via a crafted file.
CVE-2018-1123	procps-ng before version 3.3.15 is vulnerable to a denial of service in ps via mmap buffer overflow. Inbuilt protecti overflowed buffer, ensuring that the impact of this flaw is limited to a crash (temporary denial of service).
CVE-2018-1125	procps-ng before version 3.3.15 is vulnerable to a stack buffer overflow in pgrep. This vulnerability is mitigated by allocated string. When pgrep is compiled with FORTIFY (as on Red Hat Enterprise Linux and Fedora), the impact
CVE-2018-13785	In libpng 1.6.34, a wrong calculation of row_factor in the png_check_chunk_length function (pngrutil.c) may trigg by-zero while processing a crafted PNG file, leading to a denial of service.

CVE-2018-16375	An issue was discovered in OpenJPEG 2.3.0. Missing checks for header_info.height and header_info.width in the f can lead to a heap-based buffer overflow.
CVE-2018-16429	GNOME GLib 2.56.1 has an out-of-bounds read vulnerability in g_markup_parse_context_parse() in gmarkup.c, re
CVE-2018-18508	In Network Security Services (NSS) before 3.36.7 and before 3.41.1, a malformed signature can cause a crash due Service.
CVE-2018-18508	In Network Security Services (NSS) before 3.36.7 and before 3.41.1, a malformed signature can cause a crash due Service.
CVE-2018-20482	GNU Tar through 1.30, when --sparse is used, mishandles file shrinkage during read access, which allows local use loop in sparse_dump_region in sparse.c) by modifying a file that is supposed to be archived by a different user's pr
CVE-2018-25032	zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant
CVE-2018-2938	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Java DB). Supported versions that are a 8u172. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerab This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untru Java applets, such as through a web service. CVE-2018-2938 addresses CVE-2018-1313. CVSS 3.0 Base Score 9.0 impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2018-2940	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Suppor 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Easily exploitable vulnerability allows unauthenticate protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible da deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that lo comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deploy only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CV UI:R/S:U/C:L/I:N/A:N).
CVE-2018-2952	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurre Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171; JRockit: R28.3.18. Difficult to exploit vulne network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of t ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to c vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can a the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2018-2973	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JSSE). Supported 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Difficult to exploit vulnerability allows unauthenticated attac compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creatio data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typic Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the inter This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2018-3136	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Support 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated a protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful at unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vul typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that lo comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deploy only trusted code (e.g. code installed by an administrator). CVSS 3.0 Base Score 3.4 (Integrity impacts). CVSS Ve S:C/C:N/I:L/A:N).
CVE-2018-3139	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supp 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated a protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible da deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Jav code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Ja load and run only trusted code (e.g. code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).

CVE-2018-3149	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Su SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability a access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require hum attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact ad vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Jav sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Comp supplies data to the APIs. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Ve S:C/C:H/I:H/A:H).
CVE-2018-3169	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supporte 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vul Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Ja applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Jav does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g. code installed by (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I
CVE-2018-3180	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JSSE). Su Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerab network access via SSL/TLS to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulne insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized read Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Jav This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).
CVE-2018-3183	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Scripting) Java SE: 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows una via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, J vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sa and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vuln in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2018-3214	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Sound). S SE: 6u201, 7u191 and 8u182; Java SE Embedded: 8u181; JRockit: R28.3.19. Easily exploitable vulnerability allow access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulne to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0
CVE-2018-3639	Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before th known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel an Variant 4.
CVE-2018-6003	An issue was discovered in the _asn1_decode_simple_ber function in decoding.c in GNU Libtasn1 before 4.13. Un stack exhaustion and DoS.
CVE-2018-6323	The elf_object_p function in elfcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GN overflow because bfd_size_type multiplication is not used. A crafted ELF file allows remote attackers to cause a de have unspecified other impact.
CVE-2018-6759	The bfd_get_debug_link_info_1 function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as di unchecked strnlen operation. Remote attackers could leverage this vulnerability to cause a denial of service (segme
CVE-2018-6829	cipher/elgamal.c in Libgcrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintext information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). T assumption does not hold for Libgcrypt's ElGamal implementation.
CVE-2018-6954	systemd-tmpfiles in systemd through 237 mishandles symlinks present in non-terminal path components, which all arbitrary files via vectors involving creation of a directory and a file under that directory, and later replacing that di the fs.protected_symlinks sysctl is turned on.
CVE-2018-8740	In SQLite through 3.22.0, databases whose schema is corrupted using a CREATE TABLE AS statement could caus build.c and prepare.c.
CVE-2018-9234	GnuPG 2.2.4 and 2.2.5 does not enforce a configuration in which key certification requires an offline master Certif certifications that occurred only with access to a signing subkey.

CVE-2019-11191	The Linux kernel through 5.0.7, when CONFIG_IA32_AOUT is enabled and ia32_aout is loaded, allows local use (if any exist) because install_exec_creds() is called too late in load_aout_binary() in fs/binfmt_aout.c, and thus the condition when reading /proc/pid/stat. NOTE: the software maintainer disputes that this is a vulnerability because A been supported
CVE-2019-12378	An issue was discovered in ip6_ra_control in net/ipv6/ipv6_sockglue.c in the Linux kernel through 5.1.5. There is might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: This has
CVE-2019-12379	An issue was discovered in con_insert_unipair in drivers/tty/vt/consolemap.c in the Linux kernel through 5.1.5. Th ENOMEM outcome of kmalloc. NOTE: This id is disputed as not being an issue
CVE-2019-12381	An issue was discovered in ip_ra_control in net/ipv4/ip_sockglue.c in the Linux kernel through 5.1.5. There is an u allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: this is disputed
CVE-2019-12382	An issue was discovered in drm_load_edid_firmware in drivers/gpu/drm/drm_edid_load.c in the Linux kernel throu fwstr, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NO being a vulnerability because kstrdup() returning NULL is handled sufficiently and there is no chance for a NULL
CVE-2019-12455	An issue was discovered in sunxi_divs_clk_setup in drivers/clk/sunxi/clk-sunxi.c in the Linux kernel through 5.1.5 derived_name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system c an issue because ,ÄúThe memory allocation that was not checked is part of a code that only runs at boot time, befo is no possibility for an unprivileged user to control it, and no denial of service.,Äù
CVE-2019-12456	An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3sas/mpt3sas_ctl.c in local users to cause a denial of service or possibly have unspecified other impact by changing the value of ioc_num aka a "double fetch" vulnerability. NOTE: a third party reports that this is unexploitable because the doubly fetched
CVE-2019-13012	The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.60.0 creates directories using g_file_make_di NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_P NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 p permissions are used. This is similar to CVE-2019-12450.
CVE-2019-13050	Interaction between the sks-keyserver code through 1.2.0 of the SKS keyserver network, and GnuPG through 2.2.1 configuration line referring to a host on the SKS keyserver network. Retrieving data from this network may cause a Certificate Spamming Attack.
CVE-2019-13057	An issue was discovered in the server in OpenLDAP before 2.4.48. When the server administrator delegates rootDI databases but wants to maintain isolation (e.g., for multi-tenant deployments), slapd does not properly stop a rootD from another database during a SASL bind or with a proxyAuthz (RFC 4370) control. (It is not a common configur administrator and a DB administrator enjoy different levels of trust.)
CVE-2019-13565	An issue was discovered in OpenLDAP 2.x before 2.4.48. When using SASL authentication and session encryption in slapd access controls, it is possible to obtain access that would otherwise be denied via a simple bind for any ide SASL bind is completed, the sasl_ssf value is retained for all new non-SASL connections. Depending on the ACL of operations (searches, modifications, etc.). In other words, a successful authorization step completed by one user different user.
CVE-2019-13751	Uninitialized data in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentiall via a crafted HTML page.
CVE-2019-13752	Out of bounds read in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentia memory via a crafted HTML page.
CVE-2019-13753	Out of bounds read in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentia memory via a crafted HTML page.
CVE-2019-16231	drivers/net/fjes/fjes_main.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to
CVE-2019-16232	drivers/net/wireless/marvell/libertas/if_sdio.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return dereference.
CVE-2019-16233	drivers/scsi/qla2xxx/qla_os.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading t
CVE-2019-16234	drivers/net/wireless/intel/iwlwifi/pcie/trans.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return dereference.
CVE-2019-16276	Go before 1.12.10 and 1.13.x before 1.13.1 allow HTTP Request Smuggling.
CVE-2019-16276	Go before 1.12.10 and 1.13.x before 1.13.1 allow HTTP Request Smuggling.
CVE-2019-17450	find_abstract_instance in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU I a denial of service (infinite recursion and application crash) via a crafted ELF file.
CVE-2019-17451	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2. SEGV in _bfd_dwarf2_find_nearest_line in dwarf2.c, as demonstrated by nm.

CVE-2019-17594	There is a heap-based buffer over-read in the _nc_find_entry function in tinfo/comp_hash.c in the terminfo library
CVE-2019-17595	There is a heap-based buffer over-read in the fmt_entry function in tinfo/comp_hash.c in the terminfo library in ncu
CVE-2019-18276	An issue was discovered in disable_priv_mode in shell.c in GNU Bash through 5.0 patch 11. By default, if Bash is UID, it will drop privileges by setting its effective UID to its real UID. However, it does so incorrectly. On Linux a functionality, the saved UID is not dropped. An attacker with command execution in the shell can use "enable -f" f be a shared object that calls setuid() and therefore regains privileges. However, binaries running with an effective U
CVE-2019-18348	An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib in Python 3.x through 3.8.0. CRLF injec parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the host compor This is similar to the CVE-2019-9740 query string issue and the CVE-2019-9947 path string issue. (This is not exp fixed.). This is fixed in: v2.7.18, v2.7.18rc1; v3.5.10, v3.5.10rc1; v3.6.11, v3.6.11rc1, v3.6.12; v3.7.8, v3.7.8rc1, v3 v3.8.5, v3.8.6, v3.8.6rc1.
CVE-2019-19070	A memory leak in the spi_gpio_probe() function in drivers/spi/spi-gpio.c in the Linux kernel through 5.3.11 allows (memory consumption) by triggering devm_add_action_or_reset() failures, aka CID-d3b0ffa1d75d. NOTE: third p the system must have already been out of memory before the probe began
CVE-2019-19449	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can lead to slab-out-of-bounds read access in segment.c, related to init_min_max_mtime in fs/f2fs/segment.c (because the second argument to get_seg_entry is n
CVE-2019-19603	SQLite 3.30.1 mishandles certain SELECT statements with a nonexistent VIEW, leading to an application crash.
CVE-2019-19645	alter.c in SQLite through 3.30.1 allows attackers to trigger infinite recursion via certain types of self-referential vie statements.
CVE-2019-19880	exprListAppendList in window.c in SQLite 3.30.1 allows attackers to trigger an invalid pointer dereference becaus clauses of window definitions are mishandled.
CVE-2019-19906	cyrus-sasl (aka Cyrus SASL) 2.1.27 has an out-of-bounds write leading to unauthenticated remote denial-of-service packet. The OpenLDAP crash is ultimately caused by an off-by-one error in _sasl_add_string in common.c in cyru
CVE-2019-19924	SQLite 3.30.1 mishandles certain parser-tree rewriting, related to expr.c, vdbeaux.c, and window.c. This is caused handling.
CVE-2019-20218	selectExpander in select.c in SQLite 3.30.1 proceeds with WITH stack unwinding even after a parsing error.
CVE-2019-20387	repodata_schema2id in repodata.c in libsolv before 0.7.6 has a heap-based buffer over-read via a last schema whos schema.
CVE-2019-2422	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). Supported versions that are 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network a Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of t read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically i applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:
CVE-2019-2426	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Networking). Supported versions that a 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network a Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE acces to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2019-2602	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Suppor SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Easily exploitable vulnerability allows unauthenticat multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be e specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as throu (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2684	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported v 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized crea critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployment Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that c sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., throu APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I

CVE-2019-2698	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affecte exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Jav can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) an vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., cod Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/
CVE-2019-2708	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are Prior to Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infra compromise Data Store. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A
CVE-2019-2745	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are a and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to a vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sa and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vuln in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2762	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supporte 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticate protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unautho service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typical Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., throu APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:
CVE-2019-2766	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supp SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthen multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded acces to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2019-2769	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supporte 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticate protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unautho service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typical Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., throu APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:
CVE-2019-2786	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supporte 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attac protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful at unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applie running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untruste internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the sp service which supplies data to the APIs. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS A:N).
CVE-2019-2816	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supp SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthen multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. Thi APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Scor CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2019-2842	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JCE). The supported version that is affe vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. S result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0

CVE-2019-2894	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported vers 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized reac Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandb sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) an vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which su 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2019-2933	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Not deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Jav (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be ex Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2019-2945	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported v 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated a protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerabilit typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base S (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-2019-2949	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). Supported ver 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may s Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Ja Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applic 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for secur by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).
CVE-2019-2958	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized crea critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployment Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that c sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., throu APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I
CVE-2019-2962	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions t 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with ne compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients run or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service whi Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2964	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Sc (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2973	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versio 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients run or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service whi Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).

CVE-2019-2975	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported ver 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with ne compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) o vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sa and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vul in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L).
CVE-2019-2978	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported v 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients run or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service whi Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2981	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versio 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients run or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service whi Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2983	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients run or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service whi Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2987	Vulnerability in the Java SE product of Oracle Java SE (component: 2D). Supported versions that are affected are J vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. S result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0
CVE-2019-2988	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions t 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with ne compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients run or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2989	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported v 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critica accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java V applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Jav also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N).
CVE-2019-2992	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions t 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with ne compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients run or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).

CVE-2019-2999	Vulnerability in the Java SE product of Oracle Java SE (component: Javadoc). Supported versions that are affected 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks m Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically i applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted CVSS 3.0 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI
CVE-2019-3842	In systemd before v242-rc4, it was discovered that pam_systemd does not properly sanitize the environment before for an attacker, in some particular configurations, to set a XDG_SEAT environment variable which allows for com using the "allow_active" element rather than "allow_any".
CVE-2019-3859	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_pac who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3860	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads a compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-5827	Integer overflow in SQLite via WebSQL in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to po HTML page.
CVE-2019-9074	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2. SEGV in bfd_getl32 in libbfd.c, when called from pex64_get_runtime_function in pei-x86_64.c.
CVE-2020-11725	snd_ctl_elem_add in sound/core/control.c in the Linux kernel through 5.6.3 has a count=info->owner line, which la multiplication for unspecified "interesting side effects." NOTE: kernel engineers dispute this finding, because it co were added that were unfamiliar with the misuse of the info->owner field to represent data unrelated to the "owner" SNDRV_CTL_IOCTL_ELEM_ADD and SNDRV_CTL_IOCTL_ELEM_REPLACE, have been designed to misu
CVE-2020-12762	json-c through 0.14 has an integer overflow and out-of-bounds write via a large JSON file, as demonstrated by prin
CVE-2020-13435	SQLite through 3.32.0 has a segmentation fault in sqlite3ExprCodeTarget in expr.c.
CVE-2020-13631	SQLite before 3.32.0 allows a virtual table to be renamed to the name of one of its shadow tables, related to alter.c
CVE-2020-13776	systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by privileges when privileges of the 0x0 user account were intended.  **Note:** This issue exists because of an incomplete fix for CVE-2017-1000082.
CVE-2020-14155	libpcre in PCRE before 8.44 allows an integer overflow via a large number after a (?C substring.
CVE-2020-14350	It was found that some PostgreSQL extensions did not use search_path safely in their installation script. An attacke to trick an administrator into executing a specially crafted script, during the installation or update of such extension 12.4, before 11.9, before 10.14, before 9.6.19, and before 9.5.23.
CVE-2020-14556	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker wit to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized upd SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedd and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applic through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1
CVE-2020-14577	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported version 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker wit Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a sub data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxe Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (C I:N/A:N).
CVE-2020-14578	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network a Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a pa Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be explo applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Compo applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impa PR:N/UI:N/S:U/C:N/I:N/A:L).

CVE-2020-14579	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network a Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a pa Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be expl applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Compo applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impa PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14581	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions t 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker wit to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploit applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Compo applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality i AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14583	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attac protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful at in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clien applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) a vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., cod Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/
CVE-2020-14593	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions t 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than th Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulne deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulne in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted co and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in serve code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N
CVE-2020-14621	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versio 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attac protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unautho of Java SE, Java SE Embedded accessible data. Note: This vulnerability can only be exploited by supplying data to using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 B Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14779	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability ca Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified C Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JNDI). Supported version 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploit applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Compo applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality i AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14782	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized upd SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability c Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified C Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity im AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).

CVE-2020-14792	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Hotspot). Supported versi 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded acce access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CV Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).
CVE-2020-14796	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Not deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that lo comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deploy only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CV UI:R/S:U/C:L/I:N/A:N).
CVE-2020-14797	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized upd SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability c Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified C Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity im AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14798	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded acce to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java de and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). C UI:R/S:U/C:N/I:L/A:N).
CVE-2020-14803	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affecte exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, th installed by an administrator). CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N
CVE-2020-16590	A double free vulnerability exists in the Binary File Descriptor (BFD) (aka libbrd) in GNU Binutils 2.35 in the proc readelf, via a crafted file.
CVE-2020-16591	A Denial of Service vulnerability exists in the Binary File Descriptor (BFD) in GNU Binutils 2.35 due to an invalid demonstrated in readeif.
CVE-2020-16592	A use after free issue exists in the Binary File Descriptor (BFD) library (aka libbfd) in GNU Binutils 2.34 in bfd_ha can cause a denial of service via a crafted file.
CVE-2020-16593	A Null Pointer Dereference vulnerability exists in the Binary File Descriptor (BFD) library (aka libbfd), as distribu scan_unit_for_symbols, as demonstrated in addr2line, that can cause a denial of service via a crafted file.
CVE-2020-16599	A Null Pointer Dereference vulnerability exists in the Binary File Descriptor (BFD) library (aka libbfd), as distribu _bfd_elf_get_symbol_version_string, as demonstrated in nm-new, that can cause a denial of service via a crafted fi
CVE-2020-16845	Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encodin
CVE-2020-16845	Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encodin
CVE-2020-21583	An issue was discovered in hwclock.13-v2.27 allows attackers to gain escalated privlidges or execute arbitrary com the date.
CVE-2020-22218	An issue was discovered in function _libssh2_packet_add in libssh2 1.10.0 allows attackers to access out of bounds
CVE-2020-24553	Go before 1.14.8 and 1.15.x before 1.15.1 allows XSS because text/html is the default for CGI/FCGI handlers that
CVE-2020-24736	Buffer Overflow vulnerability found in SQLite3 v.3.27.1 and before allows a local attacker to cause a denial of ser
CVE-2020-24977	GNOME project libxml2 v2.9.10 has a global buffer over-read vulnerability in xmlEncodeEntitiesInternal at libxm commit 50f06b3e.

CVE-2020-25696	A flaw was found in the psql interactive terminal of PostgreSQL in versions before 13.1, before 12.5, before 11.10, 9.5.24. If an interactive psql session uses \gset when querying a compromised server, the attacker can execute arbit running psql. The highest threat from this vulnerability is to data confidentiality and integrity as well as system ava
CVE-2020-2583	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticat protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unautho service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typical Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., throu APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:
CVE-2020-2590	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported vers 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attac compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients runni sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) an vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which su 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-2593	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported v 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticat protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unautho some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Jav vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sa load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. Thi APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Scor CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-2601	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported vers 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attac compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may s Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Ja Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applic 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for secur by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-2604	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticat protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in takeove vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sa and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vul in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS v3.0 Base Score 8. impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2654	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affecte 13.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untr service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/
CVE-2020-2659	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported v 7u241 and 8u231; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker wit compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients run or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service whi Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-27216	In Eclipse Jetty versions 1.0 thru 9.4.32.v20200930, 10.0.0.alpha1 thru 10.0.0.beta2, and 11.0.0.alpha1 thru 11.0.0. temporary directory is shared between all users on that system. A collocated user can observe the process of creatin temporary directory and race to complete the creation of the temporary subdirectory. If the attacker wins the race th to the subdirectory used to unpack web applications, including their WEB-INF/lib jar files and JSP files. If any cod directory, this can lead to a local privilege escalation vulnerability.
CVE-2020-27218	In Eclipse Jetty version 9.4.0.RC0 to 9.4.34.v20201102, 10.0.0.alpha0 to 10.0.0.beta2, and 11.0.0.alpha0 to 11.0.0. enabled and requests from different clients are multiplexed onto a single connection, and if an attacker can send a r but not consumed by the application, then a subsequent request on the same connection will see that body prepende data but may inject data into the body of the subsequent request.

CVE-2020-27223	In Eclipse Jetty 9.4.6.v20170531 to 9.4.36.v20210114 (inclusive), 10.0.0, and 11.0.0 when Jetty handles a request large number of ,Äúquality,Äù (i.e. q) parameters, the server may enter a denial of service (DoS) state due to high resulting in minutes of CPU time exhausted processing those quality values.
CVE-2020-2754	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported ver 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with ne compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability ca Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified C Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2755	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported ver 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with ne compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability ca Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified C Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2756	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability ca Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified C Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2757	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability ca Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified C Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2773	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported vers 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability ca Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified C Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported version 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker with net SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited thro and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS S:U/C:N/I:N/A:L).
CVE-2020-2800	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Lightweight HTTP Serve Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthe multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untru Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVS UI:N/S:U/C:L/I:L/A:N).
CVE-2020-2803	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vul Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Ja applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator) Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).

CVE-2020-2805	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported vers 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vul Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Ja applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator) Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-28196	MIT Kerberos 5 (aka krb5) before 1.17.2 and 1.18.x before 1.18.3 allows unbounded recursion via an ASN.1-encoc asn.1/asn1_encode.c support for BER indefinite lengths lacks a recursion limit.
CVE-2020-2830	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized abil DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability ca Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified C Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-28362	Go before 1.14.12 and 1.15.x before 1.15.4 allows Denial of Service.
CVE-2020-28366	Code injection in the go command with cgo before Go 1.14.12 and Go 1.15.5 allows arbitrary code execution at bu name in a linked object file.
CVE-2020-28367	Code injection in the go command with cgo before Go 1.14.12 and Go 1.15.5 allows arbitrary code execution at bu a #cgo directive.
CVE-2020-29361	An issue was discovered in p11-kit 0.21.1 through 0.23.21. Multiple integer overflows have been discovered in the the p11-kit list command, where overflow checks are missing before calling realloc or calloc.
CVE-2020-29362	An issue was discovered in p11-kit 0.21.1 through 0.23.21. A heap-based buffer over-read has been discovered in t remote commands and the client library. When the remote entity supplies a byte array through a serialized PKCS#1 allow the reading of up to 4 bytes of memory past the heap allocation.
CVE-2020-35448	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2. occur in bfd_getl_signed_32 in libbfd.c because sh_entsize is not validated in _bfd_elf_slurp_secondary_reloc_sec
CVE-2020-35525	In SQlite 3.31.1, a potential null pointer derreference was found in the INTERSEC query processing.
CVE-2020-35527	In SQLite 3.31.1, there is an out of bounds access problem through ALTER TABLE for views that have a nested F
CVE-2020-36221	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to slapd crashes in the Certificate Exact service (schema_init.c serialNumberAndIssuerCheck).
CVE-2020-36222	A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertion failure in slapd in the saslAuthzTo valic
CVE-2020-36223	A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Values Return Filter control han free and out-of-bounds read).
CVE-2020-36224	A flaw was discovered in OpenLDAP before 2.4.57 leading to an invalid pointer free and slapd crash in the saslAu service.
CVE-2020-36225	A flaw was discovered in OpenLDAP before 2.4.57 leading to a double free and slapd crash in the saslAuthzTo pro
CVE-2020-36226	A flaw was discovered in OpenLDAP before 2.4.57 leading to a memch->bv_len miscalculation and slapd crash in denial of service.
CVE-2020-36227	A flaw was discovered in OpenLDAP before 2.4.57 leading to an infinite loop in slapd with the cancel_extop Canc
CVE-2020-36228	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Certificate List E of service.
CVE-2020-36229	A flaw was discovered in ldap_X509dn2bv in OpenLDAP before 2.4.57 leading to a slapd crash in the X.509 DN p service.
CVE-2020-36230	A flaw was discovered in OpenLDAP before 2.4.57 leading in an assertion failure in slapd in the X.509 DN parsing denial of service.
CVE-2020-36694	An issue was discovered in netfilter in the Linux kernel before 5.10. There can be a use-after-free in the packet pro sequence count is mishandled during concurrent iptables rules replacement. This could be exploited with the CAP_ namespace. NOTE: cc00bca was reverted in 5.12.
CVE-2020-8231	Due to use of a dangling pointer, libcurl 7.29.0 through 7.71.1 can use the wrong connection when sending data.

CVE-2020-8284	A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given make curl extract information about services that are otherwise private and not disclosed, for example doing port sc
CVE-2020-8285	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wil
CVE-2020-8991	vg_lookup in daemons/lvmetad/lvmetad-core.c in LVM2 2.02 mismanages memory, leading to an lvmetad memory NOTE: RedHat disputes CVE-2020-8991 as not being a vulnerability since there,Äôs no apparent route to either pr through the bug
CVE-2021-20197	There is an open race window when writing output in the following utilities in GNU binutils version 2.35 and earli utilities are run as a privileged user (presumably as part of a script updating binaries across different users), an unpr getting ownership of arbitrary files through a symlink.
CVE-2021-20229	A flaw was found in PostgreSQL in versions before 13.2. This flaw allows a user with SELECT privilege on one c columns of the table. The highest threat from this vulnerability is to confidentiality.
CVE-2021-20266	A flaw was found in RPM's hdrblobInit() in lib/header.c. This flaw allows an attacker who can modify the rpmdb t threat from this vulnerability is to system availability.
CVE-2021-20294	A flaw was found in binutils readelf 2.35 program. An attacker who is able to convince a victim using readelf to re overflow, out-of-bounds write of arbitrary data supplied by the attacker. The highest impact of this flaw is to confi
CVE-2021-22876	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an Unauthorized Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP reques
CVE-2021-22898	curl 7.7 through 7.76.1 suffers from an information disclosure when the `-t` command line option, known as `CUR used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending NEW_ENV uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal inform protocol.
CVE-2021-22924	libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse, if one of them mat config matching function did not take 'issuercert' into account and it compared the involved paths *case insensitive connections.File paths are, or can be, case sensitive on many systems but not all, and caneven vary depending on us include the 'issuer cert' which a transfer can setto qualify how to verify the server certificate.
CVE-2021-22925	curl supports the `-t` command line option, known as `CURLOPT_TELNETOPTIONS`in libcurl. This rarely used toTELNET servers.Due to flaw in the option parser for sending `NEW_ENV` variables, libcurlcould be made to pa buffer to theserver. Therefore potentially revealing sensitive internal information to theserver using a clear-text net did not call and use sscanf() correctly whenparsing the string provided by the application.
CVE-2021-22946	A user can tell curl >= 7.20.0 and <= 7.78.0 to require a successful upgrade to TLS when speaking to an IMAP, PO command line or`CURLOPT_USE_SSL` set to `CURLUSESSL_CONTROL` or `CURLUSESSL_ALL` withlibcu the server would return a properly crafted but perfectly legitimate response.This flaw would then make curl silently contrary to the instructions and expectations, exposing possibly sensitive data in clear text over the network.
CVE-2021-22947	When curl >= 7.20.0 and <= 7.78.0 connects to an IMAP or POP3 server to retrieve data using STARTTLS to upgr and send back multiple responses at once that curl caches. curl would then upgrade to TLS but not flush the in-que using and trustingthe responses it got *before* the TLS handshake as if they were authenticated.Using this flaw, it inject the fake responses, then pass-through the TLS traffic from the legitimate server and trick curl into sending da injected data comes from the TLS-protected server.
CVE-2021-23214	When the server is configured to use trust authentication with a clientcert requirement or to use cert authentication, arbitrary SQL queries when a connection is first established, despite the use of SSL certificate verification and encr
CVE-2021-23222	A man-in-the-middle attacker can inject false responses to the client's first few queries, despite the use of SSL certi
CVE-2021-27212	In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion failure in slapd can occur in the issuerAnd packet, resulting in a denial of service (daemon exit) via a short timestamp. This is related to schema_init.c and che
CVE-2021-27218	An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before 2.67.4. If g_byte_array_new_take() was bit platform, the length would be truncated modulo 2**32, causing unintended length truncation.
CVE-2021-28153	An issue was discovered in GNOME GLib before 2.66.8. When g_file_replace() is used with G_FILE_CREATE_I that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceiv attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly rema
CVE-2021-28165	In Eclipse Jetty 7.2.2 to 9.4.38, 10.0.0.alpha0 to 10.0.1, and 11.0.0.alpha0 to 11.0.1, CPU usage can reach 100% up
CVE-2021-28831	decompress_gunzip.c in BusyBox through 1.32.1 mishandles the error bit on the huft_build result pointer, with a re malformed gzip data.
CVE-2021-3200	Buffer overflow vulnerability in libsolv 2020-12-13 via the Solver * testcase_read(Pool *pool, FILE *fp, const cha *resultflagsp function at src/testcase.c: line 2334, which could cause a denial of service

CVE-2021-32028	A flaw was found in postgresql. Using an INSERT ... ON CONFLICT ... DO UPDATE command on a purpose-cra could read arbitrary bytes of server memory. The highest threat from this vulnerability is to data confidentiality.
CVE-2021-32029	A flaw was found in postgresql. Using an UPDATE ... RETURNING command on a purpose-crafted table, an auth bytes of server memory. The highest threat from this vulnerability is to data confidentiality.
CVE-2021-33061	Insufficient control flow management for the Intel(R) 82599 Ethernet Controllers and Adapters may allow an authe service via local access.
CVE-2021-33560	Libgcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to mpi_powm, and the window size is not chosen appropriately. This, for example, affects use of ElGamal in OpenPG
CVE-2021-33574	The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use th through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application
CVE-2021-33621	The cgi gem before 0.1.0.2, 0.2.x before 0.2.2, and 0.3.x before 0.3.5 for Ruby allows HTTP response splitting. Th user input either to generate an HTTP response or to create a CGI::Cookie object.
CVE-2021-33631	Integer Overflow or Wraparound vulnerability in openEuler kernel on Linux (filesystem modules) allows Forced In kernel: from 4.19.90 before 4.19.90-2401.3, from 5.10.0-60.18.0 before 5.10.0-183.0.0.
CVE-2021-33928	Buffer overflow vulnerability in function pool_installable in src/repo.h in libsolv before 0.7.17 allows attackers to c
CVE-2021-33929	Buffer overflow vulnerability in function pool_disabled_solvable in src/repo.h in libsolv before 0.7.17 allows attac
CVE-2021-33930	Buffer overflow vulnerability in function pool_installable_whatprovides in src/repo.h in libsolv before 0.7.17 allow
CVE-2021-33938	Buffer overflow vulnerability in function prune_to_recommended in src/policy.c in libsolv before 0.7.17 allows att
CVE-2021-3421	A flaw was found in the RPM package in the read functionality. This flaw allows an attacker who can convince a v or compromise an RPM repository, to cause RPM database corruption. The highest threat from this vulnerability is versions before 4.17.0-alpha.
CVE-2021-3516	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be p free. The greatest impact of this flaw is to confidentiality, integrity, and availability.
CVE-2021-3517	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is ab by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most li availability, with some potential impact to confidentiality and integrity if an attacker is able to use memory informa
CVE-2021-3518	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability.
CVE-2021-3520	There's a flaw in lz4. An attacker who submits a crafted file to an application linked with lz4 may be able to trigger memmove() on a negative size argument, causing an out-of-bounds write and/or a crash. The greatest impact of this impact to confidentiality and integrity as well.
CVE-2021-3521	There is a flaw in RPM's signature functionality. OpenPGP subkeys are associated with a primary key via a "bindi binding signature of subkeys prior to importing them. If an attacker is able to add or socially engineer another party public key, RPM could wrongly trust a malicious signature. The greatest impact of this flaw is to data integrity. To compromise an RPM repository or convince an administrator to install an untrusted RPM or public key. It is strong public keys from trusted sources.
CVE-2021-3537	A vulnerability found in libxml2 in versions before 2.9.11 shows that it did not propagate errors while parsing XM dereference. If an untrusted XML document was parsed in recovery mode and post-validated, the flaw could be use from this vulnerability is to system availability.
CVE-2021-3541	A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mec
CVE-2021-35937	A race condition vulnerability was found in rpm. A local unprivileged user could use this flaw to bypass the checks CVE-2017-7500 and CVE-2017-7501, potentially gaining root privileges. The highest threat from this vulnerability well as system availability.
CVE-2021-35938	A symbolic link issue was found in rpm. It occurs when rpm sets the desired permissions and credentials after insta use this flaw to exchange the original file with a symbolic link to a security-critical file and escalate their privileges vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-35939	It was found that the fix for CVE-2017-7500 and CVE-2017-7501 was incomplete: the check was only implemente created. A local unprivileged user who owns another ancestor directory could potentially use this flaw to gain root vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-3601	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was w class this issue as a security vulnerability. The trusted CA store should not contain anything that the user does not t github.com/openssl/openssl/issues/5236#issuecomment-119646061

CVE-2021-36222	ec_verify in kdc/kdc_preauth_ec.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.18 attackers to cause a NULL pointer dereference and daemon crash. This occurs because a return value is not properl
CVE-2021-3669	A flaw was found in the Linux kernel. Measuring usage of the shared memory does not scale with large shared mer resource exhaustion and DoS.
CVE-2021-3671	A null pointer de-reference was found in the way samba kerberos server handled missing sname in TGS-REQ (Tick authenticated user could use this flaw to crash the samba server.
CVE-2021-37322	GCC c++filt v2.26 was discovered to contain a use-after-free vulnerability via the component cplus-dem.c.
CVE-2021-37600	An integer overflow in util-linux through 2.37.1 can potentially cause a buffer overflow if an attacker were able to large number in the /proc/sysvipc/sem file.  **Note:** This is unexploitable in GNU C Library environments, and possibly in all realistic environments.
CVE-2021-3800	A flaw was found in glib before version 2.63.6. Due to random charset alias, pkexec can leak content from files ow under the right condition.
CVE-2021-38185	GNU cpio through 2.13 allows attackers to execute arbitrary code via a crafted pattern file, because of a dstring.c d of-bounds heap write. NOTE: it is unclear whether there are common cases where the pattern file, associated with t
CVE-2021-3847	An unauthorized access to the execution of the setuid file with capabilities flaw in the Linux kernel OverlayFS subs capable file from a nosuid mount into another mount. A local user could use this flaw to escalate their privileges or
CVE-2021-39686	In several functions of binder.c, there is a possible way to represent the wrong domain to SELinux due to a race co privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: A A-200688826References: Upstream kernel
CVE-2021-4023	A flaw was found in the io-workqueue implementation in the Linux kernel versions prior to 5.15-rc1. The kernel ca operation triggers the submission of new io-uring operations during a shortage of free space. This flaw allows a loc requests to possibly crash the system.
CVE-2021-40528	The ElGamal implementation in Libgcrypt before 1.9.4 allows plaintext recovery because, during interaction betwe dangerous combination of the prime defined by the receiver's public key, the generator defined by the receiver's pu exponents can lead to a cross-configuration attack against OpenPGP.
CVE-2021-4149	A vulnerability was found in btrfs_alloc_tree_b in fs/btrfs/extent-tree.c in the Linux kernel due to an improper lock local privilege may cause a denial of service (DOS) due to a deadlock problem.
CVE-2021-4204	An out-of-bounds (OOB) memory access flaw was found in the Linux kernel's eBPF due to an Improper Input Vali a special privilege to crash the system or leak internal information.
CVE-2021-42374	An out-of-bounds heap read in Busybox's unlzma applet leads to information leak and denial of service when craft This can be triggered by any applet/format that
CVE-2021-42376	A NULL pointer dereference in Busybox's hush applet leads to denial of service when processing a crafted shell co delimiter character. This may be used for DoS under very rare conditions of filtered command input.
CVE-2021-42378	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a
CVE-2021-42379	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a function
CVE-2021-42380	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a
CVE-2021-42381	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a
CVE-2021-42382	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a
CVE-2021-42384	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a function
CVE-2021-42385	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a
CVE-2021-42386	A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a

CVE-2021-42574	An issue was discovered in the Bidirectional Algorithm in the Unicode Specification through 14.0. It permits the vi sequences, which can be used to craft source code that renders different logic than the logical ordering of tokens in Adversaries can leverage this to encode source code for compilers accepting Unicode such that targeted vulnerabili reviewers. **Note:** The Unicode Consortium offers the following alternative approach to presenting this concern. An text that can affect applications that implement support for The Unicode Standard and the Unicode Bidire to text display behavior when text includes left-to-right and right-to-left characters, the visual order of tol order. Additionally, control characters needed to fully support the requirements of bidirectional text can f Unless mitigated, an adversary could craft source code such that the ordering of tokens perceived by hum processed by a compiler/interpreter/etc. The Unicode Consortium has documented this class of vulnerabi Report #36, Unicode Security Considerations. The Unicode Consortium also provides guidance on mitiga Technical Standard #39, Unicode Security Mechanisms, and in Unicode Standard Annex #31, Unicode Id specification allows applications to tailor the implementation in ways that can mitigate misleading visual Unicode Standard Annex #9, Unicode Bidirectional Algorithm.
CVE-2021-43519	Stack overflow in lua_resume of ldo.c in Lua Interpreter 5.1.0~5.4.4 allows attackers to perform a Denial of Servic
CVE-2021-43618	GNU Multiple Precision Arithmetic Library (GMP) through 6.2.1 has an mpz/inp_raw.c integer overflow and resul to a segmentation fault on 32-bit platforms.
CVE-2021-43797	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high Netty prior to version 4.1.71.Final skips control chars when they are present at the beginning / end of the header na allowed by the spec and could lead to HTTP request smuggling. Failing to do the validation might cause netty to "s to another remote system when used as proxy. This remote system can't see the invalid usage anymore, and therefo should upgrade to version 4.1.71.Final.
CVE-2021-44568	Two heap-overflow vulnerabilities exist in openSUSE/libsolv libsolv through 13 Dec 2020 in the decisionmap vari src/solver.c (line 1940 & line 1995), which could cause a remote Denial of Service.
CVE-2021-44758	Heimdal before 7.7.1 allows attackers to cause a NULL pointer dereference in a SPNEGO acceptor via a preferred_ nonzero initial_response value to send_accept.
CVE-2021-44758	Heimdal before 7.7.1 allows attackers to cause a NULL pointer dereference in a SPNEGO acceptor via a preferred_ nonzero initial_response value to send_accept.
CVE-2021-46195	GCC v12.0 was discovered to contain an uncontrolled recursion via the component libiberty/rust-demangle.c. This Denial of Service (DoS) by consuming excessive CPU and memory resources.
CVE-2021-46822	The PPM reader in libjpeg-turbo through 2.0.90 mishandles use of tjLoadImage for loading a 16-bit binary PPM fil binary PGM file into an RGB buffer. This is related to a heap-based buffer overflow in the get_word_rgb_row func
CVE-2021-46848	GNU Libtasn1 before 4.19.0 has an ETYPE_OK off-by-one array size check that affects asn1_encode_simple_der.
CVE-2021-47028	In the Linux kernel, the following vulnerability has been resolved: mt76: mt7915: fix txrate reporting Properly chec reporting. [1215.161863] Call trace: [1215.164307] cfg80211_calculate_bitrate+0x124/0x200 [cfg80211] [1215. +0x80/0xc0 [mac80211] [1215.175624] ieee80211_tx_status_ext+0x508/0x838 [mac80211] [1215.181190] mt79 [mt7915e] [1215.186580] mt7915_mac_tx_free+0x324/0x7c0 [mt7915e] [1215.191623] mt7915_queue_rx_skb+ mt76_dma_cleanup+0x7b0/0x11d0 [mt76] [1215.201276] __napi_poll+0x38/0xf8 [1215.204668] napi_workfn+0 +0x1fc/0x390 [1215.212062] worker_thread+0x48/0x4d0 [1215.215715] kthread+0x120/0x128 [1215.218935] r
CVE-2021-47037	In the Linux kernel, the following vulnerability has been resolved: ASoC: q6afe-clocks: fix reprobing of the driver example if the APR services are restarted after the firmware crash. However currently Q6afe-clocks driver will oop _probe call. Rewrite the driver to fill the clock data at runtime rather than using big static array of clocks.
CVE-2021-47105	In the Linux kernel, the following vulnerability has been resolved: ice: xsk: return xsk buffers back to pool when cl xdp_buff pointer in the internal SW ring but we never give it back to the xsk buffer pool. This means that buffers c used again. Add missing xsk_buff_free() call to the routine that is supposed to clean the entries that are left in the r used by other sockets. Also, only go through the space that is actually left to be cleaned instead of a whole ring.
CVE-2021-47131	In the Linux kernel, the following vulnerability has been resolved: net/tls: Fix use-after-free after the TLS device g active TLS offload goes down, tls_device_down is called to stop the offload and tear down the TLS context. Howe points to the TLS context, which is now deallocated. If a netdev goes up, while the connection is still active, and th retransmissions, it will lead to a use-after-free of the TLS context. This commit addresses this bug by keeping the c and implements the necessary fallbacks, so that the connection can resume in software (non-offloaded) kTLS mode encrypt all packets. The RX side already has all the necessary fallbacks, because receiving non-decrypted packets i is to block resync requests, which are normally produced after receiving non-decrypted packets. The necessary syn teardown: first the fallbacks are deployed, then the driver resources are released (it used to be possible to have a tls called TLS_RX_DEV_DEGRADED is added to indicate the fallback mode. It's used to skip the RX resync logic c objects may be released (for example, resync_async, which is allocated and freed by the driver).
CVE-2021-47193	In the Linux kernel, the following vulnerability has been resolved: scsi: pm80xx: Fix memory leak during rmmod I This would lead to memory leak during driver removal. Properly free memory when the module is removed.

CVE-2021-47200	In the Linux kernel, the following vulnerability has been resolved: drm/prime: Fix use after free in mmap with drm drops a reference to the gem object on success. If the gem object's refcount == 1 on entry to drm_gem_prime_mma and the subsequent drm_gem_object_get() will be a UAF. Fix by grabbing a reference before calling the mmap hel reference dropping was adding in commit 9786b65bc61ac ("drm/ttm: fix mmap refcounting"): "For that to work pr drm_gem_ttm_mmap() must be moved so it happens before calling obj->funcs->mmap(), otherwise the gem refcou
CVE-2021-47382	In the Linux kernel, the following vulnerability has been resolved: s390/qeth: fix deadlock during failing recovery deadlock during recovery") removed taking discipline_mutex inside qeth_do_reset(), fixing potential deadlocks. A still takes discipline_mutex and thus has the original deadlock potential. Intermittent deadlocks were seen when a q causing a race between qeth_do_reset and ccwgroup_remove. Call qeth_set_offline() directly in the qeth_do_reset(ccwgroup_set_offline(), without taking discipline_mutex.
CVE-2021-47484	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: Fix possible null pointer dereferen dereference in files "rvu_debugfs.c" and "rvu_nix.c"
CVE-2021-47489	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix even more out of bound writes fixed by: commit f23750b5b3d98653b31d4469592935ef6364ad67 Author: Thelford Williams <tdwilliamsiv@gma -0400 drm/amdgpu: fix out of bounds write but amdgpu_dm_debugfs.c contains more of the same issue so fix the r dp_max_bpc_write (Harry Wentland)
CVE-2021-47622	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: Fix a deadlock in the error handler The on a test setup: - All tags allocated - The SCSI error handler calls ufshcd_eh_host_reset_handler() - ufshcd_eh_hos ufshcd_err_handler() - ufshcd_err_handler() locks up as follows: Workqueue: ufs_eh_wq_0 ufshcd_err_handler.cfi __schedule+0x6cc/0xa94 schedule+0x12c/0x298 blk_mq_get_tag+0x210/0x480 __blk_mq_alloc_request+0x1c8/0 ufshcd_exec_dev_cmd+0x68/0x640 ufshcd_verify_dev_init+0x68/0x35c ufshcd_probe_hba+0x12c/0x1cb8 ufshcd ufshcd_reset_and_restore+0xd0/0x354 ufshcd_err_handler+0x408/0xc58 process_one_work+0x24c/0x66c worker ret_from_fork+0x10/0x30 Fix this lockup by making ufshcd_exec_dev_cmd() allocate a reserved request.
CVE-2022-0500	A flaw was found in unrestricted eBPF usage by the BPF_BTF_LOAD, leading to a possible out-of-bounds memor subsystem due to the way a user loads BTF. This flaw allows a local user to crash or escalate their privileges on the
CVE-2022-0536	Improper Removal of Sensitive Information Before Storage or Transfer in NPM follow-redirects prior to 1.14.8.
CVE-2022-1205	A NULL pointer dereference flaw was found in the Linux kernel,Äôs Amateur Radio AX.25 protocol functionality This flaw allows a local user to crash the system.
CVE-2022-1271	An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insuffic with two or more newlines where selected content and the target file names are embedded in crafted multi-line file privileged attacker to force zgrep to write arbitrary files on the system.
CVE-2022-1586	An out-of-bounds read vulnerability was discovered in the PCRE2 library in the compile_xclass_matchingpath() fu involves a unicode property matching issue in JIT-compiled regular expressions. The issue occurs because the char within JIT.
CVE-2022-1587	An out-of-bounds read vulnerability was discovered in the PCRE2 library in the get_recurse_data_length() function affects recursions in JIT-compiled regular expressions caused by duplicate data transfers.
CVE-2022-1664	Dpkg::Source::Archive in dpkg, the Debian package management system, before version 1.21.8, 1.20.10, 1.19.8, 1. vulnerability. When extracting untrusted source packages in v2 and v3 source package formats that include a debia directory traversal situations on specially crafted orig.tar and debian.tar tarballs.
CVE-2022-2196	A regression exists in the Linux Kernel within KVM: nVMX that allowed for speculative execution attacks.¬†L2 c L1 thinking it doesn't need retpolines or IBPB¬†after running L2 due to KVM (L0) advertising eIBRS support to L execute code on an indirect branch on the host machine. We recommend upgrading to Kernel 6.2 or past commit¬†
CVE-2022-23476	Nokogiri is an open source XML and HTML library for the Ruby programming language. Nokogiri `1.13.8` and `1 `xmlTextReaderExpand` in the method `Nokogiri::XML::Reader#attribute_hash`. This can lead to a null pointer ex For applications using `XML::Reader` to parse untrusted inputs, this may potentially be a vector for a denial of serv Nokogiri `>= 1.13.10`. Users may be able to search their code for calls to either `XML::Reader#attributes` or `XM they are affected.
CVE-2022-23491	Certifi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verify 2022.12.07 removes root certificates from "TrustCor" from the root store. These are in the process of being remove root certificates are being removed pursuant to an investigation prompted by media reporting that TrustCor's owner spyware. Conclusions of Mozilla's investigation can be found in the linked google group discussion.
CVE-2022-24823	Netty is an open-source, asynchronous event-driven network application framework. The package `io.netty:netty-c contains an insufficient fix for CVE-2021-21290. When Netty's multipart decoders are used local information discl temporary directory if temporary storing uploads on the disk is enabled. This only impacts applications running on vulnerability impacts code running on Unix-like systems, and very old versions of Mac OSX and Windows as they between all users. Version 4.1.77.Final contains a patch for this vulnerability. As a workaround, specify one's own DefaultHttpDataFactory.setBaseDir(...) to set the directory to something that is only readable by the current user.

CVE-2022-2509	A vulnerability found in gnutls. This security flaw happens because of a double free error occurs during verificatio function.
CVE-2022-25265	In the Linux kernel through 5.16.10, certain binary files may have the exec-all attribute if they were built in approx kernel 2.4.20). This can cause execution of bytes located in supposedly non-executable regions of a file.
CVE-2022-25313	In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting dep
CVE-2022-2625	A vulnerability was found in PostgreSQL. This attack requires permission to create non-temporary objects in at lea an administrator to create or update an affected extension in that schema, and the ability to lure or wait for a victim REPLACE or CREATE IF NOT EXISTS. Given all three prerequisites, this flaw allows an attacker to run arbitrary superuser.
CVE-2022-27672	When SMT is enabled, certain AMD processors may speculatively execute instructions using a target from the sibl potentially resulting in information disclosure.
CVE-2022-27774	An insufficiently protected credentials vulnerability exists in curl 4.9 to and include curl 7.82.0 are affected that co when follows HTTP(S) redirects is used with authentication could leak credentials to other services that exist on di
CVE-2022-27776	A insufficiently protected credentials vulnerability in fixed in curl 7.83.0 might leak authentication or cookie heade another port number.
CVE-2022-27778	A use of incorrectly resolved name vulnerability fixed in 7.83.1 might remove the wrong file when `--no-clobber` i
CVE-2022-27779	libcurl wrongly allows cookies to be set for Top Level Domains (TLDs) if thehost name is provided with a trailing cookies. curl's "cookie engine" can bebuilt with or without [Public Suffix List](https://publicsuffix.org/)awareness. rudimentary check exists to atleast prevent cookies from being set on TLDs. This check was broken if thehost nam allow arbitrary sites to set cookies that then would get sent to adifferent and unrelated site or domain.
CVE-2022-27780	The curl URL parser wrongly accepts percent-encoded URL separators like '/'when decoding the host name part of wrong host name when it is later retrieved.For example, a URL like `http://example.com%2F127.0.0.1/`, would be `http://example.com/127.0.0.1/`. This flawcan be used to circumvent filters, checks and more.
CVE-2022-27781	libcurl provides the `CURLOPT_CERTINFO` option to allow applications torequest details to be returned about a function, a malicious server could make libcurl built withNSS get stuck in a never-ending busy-loop when trying to
CVE-2022-27782	libcurl would reuse a previously created connection even when a TLS or SSHrelated option had been changed that previously used connections in a connection pool for subsequenttransfers to reuse if one of them matches the setup left out from the configuration match checks, making themmatch too easily.
CVE-2022-28321	The Linux-PAM package before 1.5.2-6.1 for openSUSE Tumbleweed allows authentication bypass for SSH login correctly restrict login if a user tries to connect from an IP address that is not resolvable via DNS. In such condition still get access. NOTE: the relevance of this issue is largely limited to openSUSE Tumbleweed and openSUSE Fac
CVE-2022-28391	BusyBox through 1.35.0 allows remote attackers to execute arbitrary code if netstat is used to print a DNS PTR rec Alternatively, the attacker could choose to change the terminal's colors.
CVE-2022-28948	An issue in the Unmarshal function in Go-Yaml v3 causes the program to crash when attempting to deserialize inva
CVE-2022-29155	In OpenLDAP 2.x before 2.5.12 and 2.6.x before 2.6.2, a SQL injection vulnerability exists in the experimental bac within an LDAP query. This can occur during an LDAP search operation when the search filter is processed, due to
CVE-2022-29824	In libxml2 before 2.9.14, several buffer handling functions in buf.c (xmlBuf*) and tree.c (xmlBuffer*) don't check out-of-bounds memory writes. Exploitation requires a victim to open a crafted, multi-gigabyte XML file. Other sof example libxslt through 1.1.35, is affected as well.
CVE-2022-30115	Using its HSTS support, curl can be instructed to use HTTPS directly insteadof using an insecure clear-text HTTP This mechanism could be bypassed if the host name in the given URL used atrailing dot while not using one when around - by having the trailing dot in the HSTS cache and *not* using thetrailing dot in the URL.
CVE-2022-30115	Using its HSTS support, curl can be instructed to use HTTPS directly insteadof using an insecure clear-text HTTP This mechanism could be bypassed if the host name in the given URL used atrailing dot while not using one when around - by having the trailing dot in the HSTS cache and *not* using thetrailing dot in the URL.
CVE-2022-3108	An issue was discovered in the Linux kernel through 5.16-rc6. kfd_parse_subtype_iolink in drivers/gpu/drm/amd/a value of kmemdup().
CVE-2022-3114	An issue was discovered in the Linux kernel through 5.16-rc6. imx_register_uart_clocks in drivers/clk/imx/clk.c la will cause the null pointer dereference.

CVE-2022-31159	The AWS SDK for Java enables Java developers to work with Amazon Web Services. A partial-path traversal issu method in the AWS S3 TransferManager component of the AWS SDK for Java v1 prior to version 1.12.261. Appli `destinationDirectory` argument, but S3 object keys are determined by the application that uploaded the objects. Th allows the caller to pass a filesystem object in the object key but contained an issue in the validation logic for the k could bypass the validation logic by including a UNIX double-dot in the bucket key. Under certain conditions, this directory from their S3 bucket that is one level up in the filesystem from their working directory. This issue,Äôs sc name prefix matches the destinationDirectory. E.g. for destination directory`/tmp/foo`, the actor can cause a downl bar`. If `com.amazonaws.services.s3.transfer.TransferManager::downloadDirectory` is used to download an untrus that bucket can be written outside of the intended destination directory. Version 1.12.261 contains a patch for this i `com.amazonaws.services.s3.transfer.TransferManager::downloadDirectory`, pass a `KeyFilter` that forbids `S3Ob return a string containing the substring `..` .
CVE-2022-3116	The Heimdal Software Kerberos 5 implementation is vulnerable to a null pointer dereferance. An attacker with net the vulnerable code path can cause the application to crash.
CVE-2022-31197	PostgreSQL JDBC Driver (PgJDBC for short) allows Java programs to connect to a PostgreSQL database using sta The PGJDBC implementation of the `java.sql.ResultRow.refreshRow()` method is not performing escaping of colu contains a statement terminator, e.g. `;`, could lead to SQL injection. This could lead to executing additional SQL c User applications that do not invoke the `ResultSet.refreshRow()` method are not impacted. User application that d underlying database that they are querying via their JDBC application may be under the control of an attacker. The into executing SQL against a table name who's column names would contain the malicious SQL and subsequently ResultSet. Note that the application's JDBC user and the schema owner need not be the same. A JDBC application database schemas owned by potentially malicious less-privileged users would be vulnerable. In that situation it may schema that causes the application to execute commands as the privileged user. Patched versions will be released a upgrade. There are no known workarounds for this issue.
CVE-2022-32208	When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw attack to go unnoticed and even allows it to inject data to the client.
CVE-2022-3358	OpenSSL supports creating a custom cipher via the legacy EVP_CIPHER_meth_new() function and associated fun in OpenSSL 3.0 and application authors are instead encouraged to use the new provider mechanism in order to imp 3.0.0 to 3.0.5 incorrectly handle legacy custom ciphers passed to the EVP_EncryptInit_ex2(), EVP_DecryptInit_ex (as well as other similarly named encryption and decryption initialisation functions). Instead of using the custom ci an equivalent cipher from the available providers. An equivalent cipher is found based on the NID passed to EVP_ supposed to represent the unique NID for a given cipher. However it is possible for an application to incorrectly pa EVP_CIPHER_meth_new(). When NID_undef is used in this way the OpenSSL encryption/decryption initialisatio being equivalent and will fetch this from the available providers. This will succeed if the default provider has been loaded that offers this cipher). Using the NULL cipher means that the plaintext is emitted as the ciphertext. Applica call EVP_CIPHER_meth_new() using NID_undef and subsequently use it in a call to an encryption/decryption init SSL/TLS are not impacted by this issue. Fixed in OpenSSL 3.0.6 (Affected 3.0.0-3.0.5).
CVE-2022-3437	A heap-based buffer overflow vulnerability was found in Samba within the GSSAPI unwrap_des() and unwrap_des Triple-DES decryption routines in the Heimdal GSSAPI library allow a length-limited write buffer overflow on ma a maliciously small packet. This flaw allows a remote user to send specially crafted malicious data to the applicatio (DoS) attack.
CVE-2022-34903	GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's GPGME) are met, allows signature forgery via injection into the status line.
CVE-2022-3515	A vulnerability was found in the Libksba library due to an integer overflow within the CRL parser. The vulnerabili execution on the target system by passing specially crafted data to the application, for example, a malicious S/MIM
CVE-2022-35252	When curl is used to retrieve and parse cookies from a HTTP(S) server, itaccepts cookies using control codes that might make the server return 400 responses. Effectively allowing a"sister site" to deny service to all siblings.
CVE-2022-3566	A vulnerability, which was classified as problematic, was found in Linux Kernel. This affects the function tcp_gets TCP Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. The id vulnerability.
CVE-2022-3567	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the functio component IPv6 Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this i to this vulnerability.
CVE-2022-36944	Scala 2.13.x before 2.13.9 has a Java deserialization chain in its JAR file. On its own, it cannot be exploited. There object deserialization within an application. In such situations, it allows attackers to erase contents of arbitrary files arbitrary code (specifically, Function0 functions) via a gadget chain.
CVE-2022-3707	A double-free memory flaw was found in the Linux kernel. The Intel GVT-g graphics driver triggers VGA card sys intel_gvt_dma_map_guest_page function. This issue could allow a local user to crash the system.
CVE-2022-37434	zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip head call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be una nodejs/node reference).

CVE-2022-40152	Those using Woodstox to parse XML data may be vulnerable to Denial of Service attacks (DOS) if DTD support is supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may su
CVE-2022-40303	An issue was discovered in libxml2 before 2.10.3. When parsing a multi-gigabyte XML document with the XML_ integer counters can overflow. This results in an attempt to access an array at a negative 2GB offset, typically leadi
CVE-2022-40304	An issue was discovered in libxml2 before 2.10.3. Certain invalid XML entity definitions can corrupt a hash table l errors. In one case, a double-free can be provoked.
CVE-2022-4129	A flaw was found in the Linux kernel's Layer 2 Tunneling Protocol (L2TP). A missing lock when clearing sk_user_ pointer dereference. A local user could use this flaw to potentially crash the system causing a denial of service.
CVE-2022-41916	Heimdal is an implementation of ASN.1/DER, PKIX, and Kerberos. Versions prior to 7.7.1 are vulnerable to a den certificate validation library, affecting the KDC (via PKINIT) and kinit (via PKINIT), as well as any third-party ap should upgrade to Heimdal 7.7.1 or 7.8. There are no known workarounds for this issue.
CVE-2022-42010	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An au and other programs that use libdbus to crash when receiving a message with certain invalid type signatures.
CVE-2022-42011	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An au and other programs that use libdbus to crash when receiving a message where an array length is inconsistent with th
CVE-2022-42012	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An au and other programs that use libdbus to crash by sending a message with attached file descriptors in an unexpected f
CVE-2022-4285	An illegal memory access flaw was found in the binutils package. Parsing an ELF file containing corrupt symbol ve service. This issue is the result of an incomplete fix for CVE-2020-16599.
CVE-2022-42898	PAC parsing in MIT Kerberos 5 (aka krb5) before 1.19.4 and 1.20.x before 1.20.1 has integer overflows that may l kadmind, or a GSS or Kerberos application server) on 32-bit platforms (which have a resultant heap-based buffer o other platforms. This occurs in krb5_pac_parse in lib/krb5/krb/pac.c. Heimdal before 7.7.1 has "a similar bug."
CVE-2022-43680	In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_Extern situations.
CVE-2022-4379	A use-after-free vulnerability was found in __nfs42_ssc_open() in fs/nfs/nfs4file.c in the Linux kernel. This flaw al
CVE-2022-4382	A use-after-free flaw caused by a race among the superblock operations in the gadgetfs Linux driver was found. It c that is running the gadgetfs side.
CVE-2022-44640	Heimdal before 7.7.1 allows remote attackers to execute arbitrary code because of an invalid free in the ASN.1 cod (KDC).
CVE-2022-45142	The fix for CVE-2022-3437 included changing memcmp to be constant time and a workaround for a compiler bug of memcmp. When these patches were backported to the heimdal-7.7.1 and heimdal-7.8.0 branches (and possibly o causing the validation of message integrity codes in gssapi/arcfour to be inverted.
CVE-2022-45868	The web-based admin console in H2 Database Engine before 2.2.220 can be started via the CLI with the argument user to specify the password in cleartext for the web admin console. Consequently, a local user (or an attacker that means) would be able to discover the password by listing processes and their arguments. NOTE: the vendor states " Passwords should never be passed on the command line and every qualified DBA or system administrator is expec fixed in 2.2.220.
CVE-2022-45873	systemd 250 and 251 allows local users to achieve a systemd-coredump deadlock by triggering a crash that has a lo in shared/elf-util.c. The exploitation methodology is to crash a binary calling the same function recursively, and pu backtrace large enough to cause the deadlock. This must be done 16 times when MaxConnections=16 is set for the
CVE-2022-45886	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_net.c has a .disconnect ver leads to a use-after-free.
CVE-2022-45887	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/usb/ttusb-dec/ttusb_dec.c has a memory l dvb_frontend_detach call.
CVE-2022-45919	An issue was discovered in the Linux kernel through 6.0.10. In drivers/media/dvb-core/dvb_ca_en50221.c, a use-a after an open, because of the lack of a wait_event.
CVE-2022-47629	Libksba before 1.6.3 is prone to an integer overflow vulnerability in the CRL signature parser.
CVE-2022-48174	There is a stack overflow vulnerability in ash.c:6030 in busybox before 1.35. In the environment of Internet of Veh command to arbitrary code execution.
CVE-2022-48554	File before 5.43 has an stack-based buffer over-read in file_copystr in funcs.c. NOTE: "File" is the name of an Ope
CVE-2022-48566	An issue was discovered in compare_digest in Lib/hmac.py in Python through 3.9.1. Constant-time-defeating optim variable in hmac.compare_digest.

CVE-2022-48566	An issue was discovered in compare_digest in Lib/hmac.py in Python through 3.9.1. Constant-time-defeating optim variable in hmac.compare_digest.
CVE-2022-48626	In the Linux kernel, the following vulnerability has been resolved: moxart: fix potential use-after-free on remove pa structure could be accessed after it was freed in moxart_remove(), so fix this by saving the base register of the devi dereference.
CVE-2022-48645	In the Linux kernel, the following vulnerability has been resolved: net: enetc: deny offload of tc-based TSN feature ENETC (taprio, cbs, gate, police) are configured through a mix of command BD ring messages and port registers: registers are a region of the ENETC memory map which are only accessible from the PCIe Physical Function. They Functions. Moreover, attempting to access these registers crashes the kernel: $ echo 1 > /sys/bus/pci/devices/0000\ [1957:ef00] type 00 class 0x020001 fsl_enetc_vf 0000:00:01.0: Adding to iommu group 15 fsl_enetc_vf 0000:00:0 fsl_enetc_vf 0000:00:01.0 eno0vf0: renamed from eth0 $ tc qdisc replace dev eno0vf0 root taprio num_tc 8 map 0 1@4 1@5 1@6 1@7 base-time 0 \ sched-entry S 0x7f 900000 sched-entry S 0x80 100000 flags 0x2 Unable to han ffff800009551a08 Internal error: Oops: 96000007 [#1] PREEMPT SMP pc : enetc_setup_tc_taprio+0x170/0x47c l Call trace: enetc_setup_tc_taprio+0x170/0x47c enetc_setup_tc+0x38/0x2dc taprio_change+0x43c/0x970 taprio_in tc_modify_qdisc+0x1fc/0x6c0 rtnetlink_rcv_msg+0x12c/0x390 Split enetc_setup_tc() into separate functions for t enetc_qos.o from being included into enetc-vf.ko, since it serves absolutely no purpose there.
CVE-2022-48655	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Harden accesses to the res descriptors by the index upon the SCMI drivers requests through the SCMI reset operations interface can potentiall driver misbehave. Add an internal consistency check before any such domains descriptors accesses.
CVE-2022-48666	In the Linux kernel, the following vulnerability has been resolved: scsi: core: Fix a use-after-free There are two .ex implementations. Both implementations use resources associated with the SCSI host. Make sure that these resource when .exit_cmd_priv is called by waiting inside scsi_remove_host() until the tag set has been freed. This commit fi == BUG: KASAN: use-a +0x27/0xd0 [ib_srp] Read of size 8 at addr ffff888100337000 by task multipathd/16727 Call Trace: <TASK> dum +0x5e/0x5db kasan_report+0xab/0x120 srp_exit_cmd_priv+0x27/0xd0 [ib_srp] scsi_mq_exit_request+0x4d/0x70 __blk_mq_free_map_and_rqs+0x6e/0x100 blk_mq_free_tag_set+0x2b/0x160 scsi_host_dev_release+0xf3/0x1a0 +0xa5/0x120 device_release+0x54/0xe0 kobject_put+0xa5/0x120 scsi_device_dev_release_usercontext+0x4c1/0x device_release+0x54/0xe0 kobject_put+0xa5/0x120 scsi_disk_release+0x3f/0x50 device_release+0x54/0xe0 kobje +0x17f/0x1b0 device_release+0x54/0xe0 kobject_put+0xa5/0x120 dm_put_table_device+0xa3/0x160 [dm_mod] free_priority_group+0xd8/0x110 [dm_multipath] free_multipath+0x94/0xe0 [dm_multipath] dm_table_destroy+0x +0x196/0x350 [dm_mod] dev_remove+0x10c/0x160 [dm_mod] ctl_ioctl+0x2c2/0x590 [dm_mod] dm_ctl_ioctl+0 +0xb4/0xf0 dm_ctl_ioctl+0x5/0x10 [dm_mod] __x64_sys_ioctl+0xb4/0xf0 do_syscall_64+0x3b/0x90 entry_SYS
CVE-2022-48674	In the Linux kernel, the following vulnerability has been resolved: erofs: fix pcluster use-after-free on UP platform disabled, KASAN reports as below: ========== free in __mutex_lock+0xe5/0xc30 Read of size 8 at addr ffff8881094223f8 by task stress/7789 CPU: 0 PID: 7789 g0d53d2e882f9 #3 Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011 Call Trace: <TASK> .. __mutex_lock +0x8ce/0x1560 .. z_erofs_readahead+0x31c/0x580 .. Freed by task 7787 kasan_save_stack+0x1e/0x40 kasan_set_ +0x20/0x40 __kasan_slab_free+0x10c/0x190 kmem_cache_free+0xed/0x380 rcu_core+0x3d5/0xc90 __do_softirq creation: kasan_save_stack+0x1e/0x40 __kasan_record_aux_stack+0x97/0xb0 call_rcu+0x3d/0x3f0 erofs_shrink_ +0xdc/0x170 shrink_slab.constprop.0+0x296/0x530 drop_slab+0x1c/0x70 drop_caches_sysctl_handler+0x70/0x8 vfs_write+0x555/0x6c0 ksys_write+0xbe/0x160 do_syscall_64+0x3b/0x90 The root cause is that erofs_workgroup it causes a race that the pcluster reuses unexpectedly before freeing. Since UP platforms are quite rare now, such pa specific-designed path directly instead.
CVE-2022-48708	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference pcs_set_mux(). pinmux_generic_get_function() can return NULL and the pointer "function" was dereferenced with Verification Center (linuxtesting.org) with SVACE.

CVE-2022-48781	In the Linux kernel, the following vulnerability has been resolved: crypto: af_alg - get rid of alg_memory_allocated not seem to be really used. alg_proto does have a .memory_allocated field, but no corresponding .sysctl_mem. This true, but all sk_prot_mem_limits() users will trigger a NULL dereference [1]. THis was not a problem until SO_RE protection fault, probably for non-canonical address 0xdffffc0000000001: 0000 [#1] PREEMPT SMP KASAN KA [0x0000000000000008-0x000000000000000f] CPU: 1 PID: 3591 Comm: syz-executor153 Not tainted 5.17.0-rc3- Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 RIP: 0010:s [inline] RIP: 0010:sock_reserve_memory+0x1d7/0x330 net/core/sock.c:1000 Code: 08 00 74 08 48 89 ef e8 27 20 c5 08 48 89 e8 48 c1 e8 03 48 b9 00 00 00 00 00 fc ff df <80> 3c 08 00 74 08 48 89 ef e8 fb 1f bb f9 48 8b 6d 00 4 EFLAGS: 00010202 RAX: 0000000000000001 RBX: ffff88814aabc000 RCX: dffffc0000000000 RDX: 00000000 RDI: ffffffff90e18120 RBP: 0000000000000008 R08: dffffc0000000000 R09: fffffbfff21c3025 R10: fffffbfff21c3 ffffffff8d109840 R13: 0000000000001002 R14: 0000000000000001 R15: 0000000000000001 FS: 0000555556e08 knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fc74416f130 CR3: 00000000003506e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000 DR7: 0000000000000400 Call Trace: <TASK> sock_setsockopt+0x14a9/0x3a30 net/core/sock.c:1446 __sys_setso __do_sys_setsockopt net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsock do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x44/0xd0 arch/x86/entry/common.c:80 entry RIP: 0033:0x7fc7440fddc9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 15 00 00 90 48 89 f8 48 89 f7 48 89 d6 4 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffe98f07968 EFLAGS: 00 RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007fc7440fddc9 RDX: 0000000000000049 RSI: 0000000 RBP: 0000000000000000 R08: 0000000000000004 R09: 00007ffe98f07990 R10: 0000000020000000 R11: 00000 R13: 00007ffe98f079a0 R14: 00007ffe98f079e0 R15: 0000000000000000 </TASK> Modules linked in: ---[end tr 0010:sk_prot_mem_limits include/net/sock.h:1523 [inline] RIP: 0010:sock_reserve_memory+0x1d7/0x330 net/cor ef e8 27 20 bb f9 4c 03 7c 24 10 48 8b 6d 00 48 83 c5 08 48 89 e8 48 c1 e8 03 48 b9 00 00 00 00 00 fc ff df <80> 3 48 8b 6d 00 4c 89 ff 48 RSP: 0018:ffffc90001f1fb68 EFLAGS: 00010202 RAX: 0000000000000001 RBX: ffff888 RDX: 0000000000000001 RSI: 0000000000000008 RDI: ffffffff90e18120 RBP: 0000000000000008 R08: dffffc0 R10: fffffbfff21c3025 R11: 0000000000000000 R12: ffffffff8d109840 R13: 0000000000001002 R14: 0000000000 FS: 0000555556e08300(0000) GS:ffff8880b9b00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 00 00007fc74416f130 CR3: 0000000073d9e000 CR4: 00000000003506e0 DR0: 0000000000000000 DR1: 00000000
CVE-2022-48791	In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free for aborted TM occur if a TMF sas_task is aborted before we handle the IO completion in mpi_ssp_completion(). The abort occurs SAS_TASK_STATE_ABORTED flag is set and the sas_task is freed in pm8001_exec_internal_tmf_task(). Howev O completion still thinks that the sas_task is available. Fix this by clearing the ccb->task if the TMF times out - the pointer is cleared.
CVE-2022-48792	In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free for aborted SSP may occur if a sas_task is aborted by the upper layer before we handle the I/O completion in mpi_ssp_completion(following are the two steps in handling those I/O completions: - Call complete() to inform the upper layer handler o resources associated with the sas_task in pm8001_ccb_task_free() call. When complete() is called, the upper layer touch the associated sas_task afterwards, but we do so in the pm8001_ccb_task_free() call. Fix by swapping the co ordering.
CVE-2022-48814	In the Linux kernel, the following vulnerability has been resolved: net: dsa: seville: register the mdiobus under dev ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bu when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiobus wa VSC9959 switch is a platform device, so the initial set of constraints that I thought would cause this (I2C or SPI bu do not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove fro the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumer shutdown. So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the use devres at all. The seville driver has a code structure that could accommodate both the mdiobus_unregister and r dependency upon mscc_miim_setup() from mdio-mscc-miim.c, which calls devm_mdiobus_alloc_size() on its beh exporting yet one more symbol mscc_miim_teardown(), let's work with devres and replace of_mdiobus_register wi devres, we can ensure that devres doesn't free a still-registered bus (it either runs both callbacks, or none).
CVE-2022-48816	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: lock against ->sock changing during asynchronously unless ->recv_mutex is held. So it is important to hold that mutex. Otherwise a sysfs read can trigg ("SUNRPC: Check if the xprt is connected before handling sysfs reads") appears to attempt to fix this problem, but

CVE-2022-48818	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mv88e6xxx: don't use devres for mdiob ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bu panic when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiob mv88e6xxx is an MDIO device, so the initial set of constraints that I thought would cause this (I2C or SPI buses w not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove from - the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumer on shutdown. systemd-shutdown[1]: Powering off. mv88e6085 0x0000000008b96000:00 sw_gl0: Link is Down fs group 7 fsl-mc dpbp.8: Removing from iommu group 7 ----------[cut here]---------- kernel BUG at drivers/net/p BUG: 0 [#1] PREEMPT SMP Modules linked in: CPU: 0 PID: 1 Comm: systemd-shutdow Not tainted 5.16.5-0004 +0x44/0x50 lr : devm_mdiobus_free+0x10/0x20 Call trace: mdiobus_free+0x44/0x50 devm_mdiobus_free+0x10/0 __device_release_driver+0x190/0x220 device_release_driver_internal+0xac/0xb0 device_links_unbind_consumers +0x4c/0x220 device_release_driver_internal+0xac/0xb0 device_links_unbind_consumers+0xd4/0x100 __device_r device_release_driver+0x28/0x40 bus_remove_device+0x118/0x124 device_del+0x174/0x420 fsl_mc_device_rem +0xc/0x20 device_for_each_child+0x58/0xa0 dprc_remove+0x90/0xb0 fsl_mc_driver_remove+0x20/0x5c __devi device_release_driver+0x28/0x40 bus_remove_device+0x118/0x124 device_del+0x174/0x420 fsl_mc_bus_remov +0xc/0x1c platform_shutdown+0x20/0x30 device_shutdown+0x154/0x330 kernel_power_off+0x34/0x6c __do_sy +0x20/0x30 invoke_syscall.constprop.0+0x4c/0xe0 do_el0_svc+0x4c/0x150 el0_svc+0x24/0xb0 el0t_64_sync_ha So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the mdiobus a at all. The Marvell driver already has a good structure for mdiobus removal, so just plug in mdiobus_free and get ri
CVE-2022-48826	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: Fix deadlock on DSI device attach erro with host device's lock held. Un-registering host in "device attach" error path (ex: probe retry) will result in deadlo DSI display. Startup Call trace: [35.043036] rt_mutex_slowlock.constprop.21+0x184/0x1b8 [35.043048] mutex_l device_del+0x4c/0x3e8 [35.043075] device_unregister+0x20/0x40 [35.043082] mipi_dsi_remove_device_fn+0x +0x68/0xb0 [35.043105] mipi_dsi_host_unregister+0x40/0x90 [35.043115] vc4_dsi_host_attach+0xf0/0x120 [vc +0x30/0x48 [35.043209] tc358762_probe+0x128/0x164 [tc358762] [35.043225] mipi_dsi_drv_probe+0x28/0x38 [35.043244] __driver_probe_device+0x80/0xe8 [35.043254] driver_probe_device+0xb8/0x118 [35.043263] __d bus_for_each_drv+0x84/0xd8 [35.043281] __device_attach+0xf0/0x150 [35.043290] device_initial_probe+0x1c/ +0xa4/0xb0 [35.043308] deferred_probe_work_func+0xa0/0xe0 [35.043318] process_one_work+0x254/0x700 [[35.043339] kthread+0x19c/0x1a8 [35.043348] ret_from_fork+0x10/0x20 Shutdown Call trace: [365.565417] Ca +0x148/0x200 [365.565452] __schedule+0x340/0x9c8 [365.565467] schedule+0x48/0x110 [365.565479] schedu wait_for_completion+0xac/0x138 [365.565509] __flush_work+0x218/0x4e0 [365.565523] flush_work+0x1c/0x2 +0x68/0x158 [365.565550] device_shutdown+0x24/0x348 [365.565561] kernel_restart_prepare+0x40/0x50 [365 [365.565591] __do_sys_reboot+0x10c/0x220 [365.565605] __arm64_sys_reboot+0x2c/0x38 [365.565619] invol el0_svc_common.constprop.3+0xfc/0x120 [365.565648] do_el0_svc+0x2c/0x90 [365.565661] el0_svc+0x4c/0xf +0x90/0xb8 [365.565682] el0t_64_sync+0x180/0x184
CVE-2022-48833	In the Linux kernel, the following vulnerability has been resolved: btrfs: skip reserved bytes warning on unmount a changes made by commit c2e39305299f01 ("btrfs: clear extent buffer uptodate when we fail to write it") and its fol ("btrfs: check WRITE_ERR when trying to read an extent buffer"), we can now end up not cleaning up space reser transaction abort happens, as well as not cleaning up still dirty extent buffers. This happens because if writeback fo have cleared the bit EXTENT_BUFFER_UPTODATE from the extent buffer and we have also set the bit EXTENT when trying to free the log tree with free_log_tree(), which iterates over the tree, we can end up getting an -EIO err read_extent_buffer_pages() returns -EIO if an extent buffer does not have EXTENT_BUFFER_UPTODATE set an bit set. Getting that -EIO means that we return immediately as we can not iterate over the entire tree. In that case w extent buffer in the respective block group and space_info object. When this happens we get the following traces w BTRFS: error (device dm-0) in cleanup_transaction:1913: errno=-5 IO failure [174957.286497] BTRFS: error (dev errno=-5 IO failure [174957.399379] ----------[cut here]---------- [174957.402497] WARNING: CPU: 2 PID: 3 btrfs_put_block_group+0x77/0xb0 [btrfs] [174957.407523] Modules linked in: btrfs overlay dm_zero (...) [174957 umount Tainted: G W 5.16.0-rc5-btrfs-next-109 #1 [174957.426689] Hardware name: QEMU Standard PC (i440F g155821a1990b-prebuilt.qemu.org 04/01/2014 [174957.428716] RIP: 0010:btrfs_put_block_group+0x77/0xb0 [bt bd (...) [174957.432867] RSP: 0018:ffffb70d41cffdd0 EFLAGS: 00010206 [174957.433632] RAX: 000000000000 ffff8b0758edd1c8 [174957.434689] RDX: 0000000000000001 RSI: ffffffffc0b467e7 RDI: ffff8b0758edd000 [174 0000000000000000 R09: 0000000000000000 [174957.437114] R10: 0000000000000246 R11: 000000000000000 R13: ffff8b09c3848198 R14: ffff8b0758edd188 R15: dead000000000100 [174957.439317] FS: 00007f328fb8280 knlGS:0000000000000000 [174957.440402] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [174957.441 CR3: 0000000404f4e005 CR4: 0000000000370ee0 [174957.442117] DR0: 0000000000000000 DR1: 000000000 [174957.443076] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [174957.443948] C [174957.444538] btrfs_free_block_groups+0x255/0x3c0 [btrfs] [174957.445238] close_ctree+0x301/0x357 [btrfs] +0x16c/0x290 [174957.446250] generic_shutdown_super+0x74/0x120 [174957.446832] kill_anon_super+0x14/0x +0x12/0x20 [btrfs] [174957.447890] deactivate_locked_super+0x31/0xa0 [174957.448440] cleanup_mnt+0x147/0 +0x5c/0xa0 [174957.449336] exit_to_user_mode_prepare+0x1e5/0x1f0 [174957.449934] syscall_exit_to_user_mo do_syscall_64+0x48/0xc0 [174957.450980] entry_SYSCALL_64_after_hwframe+0x44/0xae [174957.451605] RI Code: 03 0c 00 f7 (...) [174957.454320] RSP: 002b:00007fff13564ec8 EFLAGS: 00000246 ORIG_RAX: 000000 0000000000000000 RBX: 00007f328feea264 RCX: 00007f328fdc4a97 [174957.456131] RDX: 000000000000000
CVE-2022-48852	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: hdmi: Unregister codec device on unbi device but we don't unregister it on unbind, leading to a device leakage. Unregister our device at unbind.
CVE-2022-48859	In the Linux kernel, the following vulnerability has been resolved: net: marvell: prestera: Add missing of_node_pu This node pointer is returned by of_find_compatible_node() with refcount incremented. Calling of_node_put() to a

CVE-2022-4886	Ingress-nginx `path` sanitization can be bypassed with `log_format` directive.
CVE-2023-0361	A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side encrypted in the RSA ciphertext across a network in a Bleichenbacher style attack. To achieve a successful decrypt amount of specially crafted messages to the vulnerable server. By recovering the secret from the ClientKeyExchan decrypt the application data exchanged over that connection.
CVE-2023-0458	A speculative pointer dereference problem exists in the Linux Kernel on the do_prlimit() function. The resource ar and is used in pointer arithmetic for the 'rlim' variable and can be used to leak the contents. We recommend upgrad commit¬†739790605705ddcf18f21782b9c99ad7d53a8c11
CVE-2023-0459	Copy_from_user on 64-bit versions of the Linux kernel does not implement the __uaccess_begin_nospec allowing check and pass a kernel pointer to copy_from_user(). This would allow an attacker to leak information. We recomm commit¬†74e19ef0ff8061ef55957c3abd71614ef0f42f47
CVE-2023-0461	There is a use-after-free vulnerability in the Linux Kernel which can be exploited to achieve local privilege escalati configuration flag CONFIG_TLS¬†or CONFIG_XFRM_ESPINTCP¬†has to be configured, but the operation doe is a use-after-free bug of icsk_ulp_data¬†of a struct inet_connection_sock. When CONFIG_TLS¬†is enabled, user tls_context) on a connected tcp socket. The context is not cleared if this socket is disconnected and reused as a liste listener, the context is inherited and vulnerable. The setsockopt¬†TCP_ULP¬†operation does not require any privi commit¬†2c02d41d71f90a5168391b6a5f2954112ba2307c
CVE-2023-0597	A flaw possibility of memory leak in the Linux kernel cpu_entry_area mapping of X86 CPU data to memory was f exception stack(s) or other important data. A local user could use this flaw to get access to some important data wit
CVE-2023-1073	A memory corruption flaw was found in the Linux kernel,Äôs human interface device (HID) subsystem in how a u allows a local user to crash or potentially escalate their privileges on the system.
CVE-2023-1074	A memory leak flaw was found in the Linux kernel's Stream Control Transmission Protocol. This issue may occur service and someone connects to this service. This could allow a local user to starve resources, causing a denial of
CVE-2023-1075	A flaw was found in the Linux Kernel. The tls_is_tx_ready() incorrectly checks for list emptiness, potentially acces leaking the last byte of the confused field that overlaps with rec->tx_ready.
CVE-2023-1078	A flaw was found in the Linux Kernel in RDS (Reliable Datagram Sockets) protocol. The rds_rm_zerocopy_callba causing a type confusion. Local user can trigger this with rds_message_put(). Type confusion leads to `struct rds_m something else that is potentially controlled by local user. It is known how to trigger this, which causes an out of bo
CVE-2023-1079	A flaw was found in the Linux kernel. A use-after-free may be triggered in asus_kbd_backlight_set when plugging which advertises itself as an Asus device. Similarly to the previous known CVE-2023-25012, but in asus devices, t controller while the device is disconnecting, triggering a use-after-free on the struct asus_kbd_leds *led structure. A to cause memory corruption with controlled data.
CVE-2023-1118	A flaw use after free in the Linux kernel integrated infrared receiver/transceiver driver was found in the way user d flaw to crash the system or potentially escalate their privileges on the system.
CVE-2023-1192	A use-after-free flaw was found in smb2_is_status_io_timeout() in CIFS in the Linux Kernel. After CIFS transfers local variable points to the memory region, and if the system call frees it faster than CIFS uses it, CIFS will access service.
CVE-2023-1281	Use After Free vulnerability in Linux kernel traffic control index filter (tcindex) allows Privilege Escalation.¬†The while packets are traversing, which will cause a use-after-free when 'tcf_exts_exec()' is called with the destroyed tc vulnerability to elevate its privileges to root. This issue affects Linux Kernel: from 4.14 before git commit ee05917
CVE-2023-1513	A flaw was found in KVM. When calling the KVM_GET_DEBUGREGS ioctl, on 32-bit systems, there might be s kvm_debugregs structure that could be copied to userspace, causing an information leak.
CVE-2023-1579	Heap based buffer overflow in binutils-gdb/bfd/libbfd.c in bfd_getl64.
CVE-2023-1611	A use-after-free flaw was found in btrfs_search_slot in fs/btrfs/ctree.c in btrfs in the Linux Kernel.This flaw allows cause a kernel information lea
CVE-2023-1670	A flaw use after free in the Linux kernel Xircom 16-bit PCMCIA (PC-card) Ethernet driver was found.A local user potentially escalate their privileges on the system.
CVE-2023-1829	A use-after-free vulnerability in the Linux Kernel traffic control index filter (tcindex) can be exploited to achieve lo tcindex_delete function which does not properly deactivate filters in case of a perfect hashes while deleting the und to double freeing the structure.¬†A local attacker user can use this vulnerability to elevate its privileges to root. We 8c710f75256bb3cf05ac7b1672c82b92c43f3d28.
CVE-2023-1855	A use-after-free flaw was found in xgene_hwmon_remove in drivers/hwmon/xgene-hwmon.c in the Hardware Mon This flaw could allow a local attacker to crash the system due to a race problem. This vulnerability could even lead
CVE-2023-1859	A use-after-free flaw was found in xen_9pfs_front_removet in net/9p/trans_xen.c in Xen transport for 9pfs in the L attacker to crash the system due to a race problem, possibly leading to a kernel information leak.

CVE-2023-1872	A use-after-free vulnerability in the Linux Kernel io_uring system can be exploited to achieve local privilege escal the presence of ctx->uring_lock which can lead to a Use-After-Free vulnerability due a race condition with fixed fi upgrading past commit da24142b1ef9fd5d36b76e36bab328a5b27523e8.
CVE-2023-1989	A use-after-free flaw was found in btsdio_remove in drivers\bluetooth\btsdio.c in the Linux Kernel. In this flaw, a may cause a race problem leading to a UAF on hdev devices.
CVE-2023-1990	A use-after-free flaw was found in ndlc_remove in drivers/nfc/st-nci/ndlc.c in the Linux Kernel. This flaw could al race problem.
CVE-2023-1998	The Linux kernel allows userspace processes to enable mitigations by calling prctl with PR_SET_SPECULATION feature as well as by using seccomp. We had noticed that on VMs of at least one major cloud provider, the kernel s attacks in some cases even after enabling the spectre-BTI mitigation with prctl. The same behavior can be observed the mitigation to IBRS on boot command line. This happened because when plain IBRS was enabled (not enhanced determined that STIBP was not needed. The IBRS bit implicitly protects against cross-thread branch target injectio bit was cleared on returning to userspace, due to performance reasons, which disabled the implicit STIBP and left u branch target injection against which STIBP protects.
CVE-2023-20860	Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "**" as a pattern in Spring Security configu mismatch in pattern matching between Spring Security and Spring MVC, and the potential for a security bypass.
CVE-2023-20861	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsuppo provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.
CVE-2023-21102	In __efi_rt_asm_wrapper of efi-rt-wrapper.S, there is a possible bypass of shadow stack protection due to a logic er escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitatio kernelAndroid ID: A-260821414References: Upstream kernel
CVE-2023-2162	A use-after-free vulnerability was found in iscsi_sw_tcp_session_create in drivers/scsi/iscsi_tcp.c in SCSI sub-com attacker could leak kernel internal information.
CVE-2023-2163	Incorrect verifier pruning¬†in BPF in Linux Kernel¬†>=5.4¬†leads to unsafe code paths being incorrectly marked kernel memory, lateral privilege escalation, and container escape.
CVE-2023-2194	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "c number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of dma_buffer. This crash the system or potentially achieve code execution.
CVE-2023-22025	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, product of Ora versions that are affected are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols GraalVM for JDK, Oracle GraalVM Enterprise Edition,. Successful attacks of this vulnerability can result in unaut of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, accessible data. Note: This vuln the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also appli running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., c the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H
CVE-2023-22067	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: C are Oracle Java SE: 8u381, 8u381-perf; Oracle GraalVM Enterprise Edition: 20.3.11 and 21.3.7. Easily exploitable with network access via CORBA to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful a unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessi exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applicatio a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:
CVE-2023-22081	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Orac versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: T typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run un internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CV I:N/A:L).
CVE-2023-2283	A vulnerability was found in libssh, where the authentication check of the connecting client can be bypassed in the memory allocation problems. This issue may happen if there is insufficient memory or the memory usage is limited `rc,` which is initialized to SSH_ERROR and later rewritten to save the return value of the function call `pki_key_c variable is not changed between this point and the cryptographic verification. Therefore any error between them ca
CVE-2023-22998	In the Linux kernel before 6.0.3, drivers/gpu/drm/virtio/virtgpu_object.c misinterprets the drm_gem_shmem_get_s in the error case, whereas it is actually an error pointer).
CVE-2023-23003	In the Linux kernel before 5.16, tools/perf/util/expr.c lacks a check for the hashmap__new return value.

CVE-2023-23039	An issue was discovered in the Linux kernel through 6.2.0-rc2. drivers/tty/vcc.c has a race condition and resultant u attacker removes a VCC device while calling open(), aka a race condition between vcc_open() and vcc_remove().
CVE-2023-23559	In rndis_query_oid in drivers/net/wireless/rndis_wlan.c in the Linux kernel through 6.1.5, there is an integer overfl
CVE-2023-2454	schema_element defeats protective search_path changes; It was found that certain database calls in PostgreSQL co database-level privileges to execute arbitrary code.
CVE-2023-2455	Row security policies disregard user ID changes after inlining; PostgreSQL could permit incorrect policies to be ap policies are used and a given query is planned under one role and then executed under other roles. This scenario ca when a common user and query is planned initially and then re-used across multiple SET ROLEs. Applying an inc otherwise-forbidden reads and modifications. This affects only databases that have used CREATE POLICY to defi
CVE-2023-24998	Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the with a malicious upload or series of uploads. Note that, like all of the file upload limits, the new configuration optio enabled by default and must be explicitly configured.
CVE-2023-25012	The Linux kernel through 6.1.9 has a Use-After-Free in bigben_remove in drivers/hid/hid-bigbenff.c via a crafted U remain registered for too long.
CVE-2023-25613	An LDAP Injection vulnerability exists in the¬†LdapIdentityBackend of Apache Kerby before 2.0.3.¬†
CVE-2023-2602	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use error, which can exhaust the process memory.
CVE-2023-2603	A vulnerability was found in libcap. This issue occurs in the _libcap_strdup() function and can lead to an integer ov
CVE-2023-26159	Versions of the package follow-redirects before 1.15.4 are vulnerable to Improper Input Validation due to the impr function. When new URL() throws an error, it can be manipulated to misinterpret the hostname. An attacker could malicious site, potentially leading to information disclosure, phishing attacks, or other security breaches.
CVE-2023-26545	In the Linux kernel before 6.1.13, there is a double free in net/mpls/af_mpls.c upon an allocation failure (for registe during the renaming of a device.
CVE-2023-27533	A vulnerability in input validation exists in curl <8.0 during communication using the TELNET protocol may allow user name and "telnet options" during server negotiation. The lack of proper input scrubbing allows an attacker to s without the application's intent. This vulnerability could be exploited if an application allows user input, thereby en the system.
CVE-2023-27535	An authentication bypass vulnerability exists in libcurl <8.0.0 in the FTP connection reuse feature that can result in subsequent transfers. Previously created connections are kept in a connection pool for reuse if they match the curre such as CURLOPT_FTP_ACCOUNT, CURLOPT_FTP_ALTERNATIVE_TO_USER, CURLOPT_FTP_SSL_CC included in the configuration match checks, causing them to match too easily. This could lead to libcurl using the w potentially allowing unauthorized access to sensitive information.
CVE-2023-27536	An authentication bypass vulnerability exists libcurl <8.0.0 in the connection reuse feature which can reuse previou incorrect user permissions due to a failure to check for changes in the CURLOPT_GSSAPI_DELEGATION option negotiate/GSSAPI transfers and could potentially result in unauthorized access to sensitive information. The safest CURLOPT_GSSAPI_DELEGATION option has been changed.
CVE-2023-27538	An authentication bypass vulnerability exists in libcurl prior to v8.0.0 where it reuses a previously established SSH option was modified, which should have prevented reuse. libcurl maintains a pool of previously used connections t configurations match. However, two SSH settings were omitted from the configuration check, allowing them to ma an inappropriate connection.
CVE-2023-28321	An improper certificate validation vulnerability exists in curl <v8.1.0 in the way it supports matching of wildcard p Name" in TLS server certificates. curl can be built to use its own name matching function for TLS rather than one p wildcard matching function would match IDN (International Domain Name) hosts incorrectly and could as a result mismatch. IDN hostnames are converted to puny code before used for certificate checks. Puny coded names always to pattern match, but the wildcard check in curl could still check for `x*`, which would match even though the IDN resembling an `x`.
CVE-2023-28322	An information disclosure vulnerability exists in curl <v8.1.0 when doing HTTP(S) transfers, libcurl might erroneo (`CURLOPT_READFUNCTION`) to ask for data to send, even when the `CURLOPT_POSTFIELDS` option has wasused to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to m or use memory after free or similar in the second transfer. The problem exists in the logic for a reused handle when a POST.
CVE-2023-28328	A NULL pointer dereference flaw was found in the az6027 driver in drivers/media/usb/dev-usb/az6027.c in the Lin not checked properly before transferring into the device. This flaw allows a local user to crash the system or potent
CVE-2023-28466	do_tls_getsockopt in net/tls/tls_main.c in the Linux kernel through 6.2.6 lacks a lock_sock call, leading to a race co NULL pointer dereference).

CVE-2023-28484	In libxml2 before 2.10.4, parsing of certain invalid XSD schemas can lead to a NULL pointer dereference and subs xmlSchemaFixupComplexType in xmlschemas.c.
CVE-2023-29469	An issue was discovered in libxml2 before 2.10.4. When hashing empty dict strings in a crafted XML document, x non-deterministic values, leading to various logic and memory errors, such as a double free. This behavior occurs b of an empty string, and any value is possible (not solely the '\0' value).
CVE-2023-2985	A use after free flaw was found in hfsplus_put_super in fs/hfsplus/super.c in the Linux Kernel. This flaw could allo problem.
CVE-2023-30456	An issue was discovered in arch/x86/kvm/vmx/nested.c in the Linux kernel before 6.2.8. nVMX on x86_64 lacks c
CVE-2023-30772	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/power/supply/da9150-cha unplugs a device.
CVE-2023-31081	An issue was discovered in drivers/media/test-drivers/vidtv/vidtv_bridge.c in the Linux kernel 6.2. There is a NUL vidtv_mux_stop_thread. In vidtv_stop_streaming, after dvb->mux=NULL occurs, it executes vidtv_mux_stop_thre
CVE-2023-31083	An issue was discovered in drivers/bluetooth/hci_ldisc.c in the Linux kernel 6.2. In hci_uart_tty_ioctl, there is a rac and HCIUARTGETPROTO. HCI_UART_PROTO_SET is set before hu->proto is set. A NULL pointer dereferenc
CVE-2023-3141	A use-after-free flaw was found in r592_remove in drivers/memstick/host/r592.c in media access in the Linux Kern the system at device disconnect, possibly leading to a kernel information leak.
CVE-2023-3161	A flaw was found in the Framebuffer Console (fbcon) in the Linux Kernel. When providing font->width and font-> since there are no checks in place, a shift-out-of-bounds occurs leading to undefined behavior and possible denial o
CVE-2023-3220	An issue was discovered in the Linux kernel through 6.1-rc8. dpu_crtc_atomic_check in drivers/gpu/drm/msm/disp value of kzalloc() and will cause the NULL Pointer Dereference.
CVE-2023-32269	An issue was discovered in the Linux kernel before 6.1.11. In net/netrom/af_netrom.c, there is a use-after-free beca connected AF_NETROM socket. However, in order for an attacker to exploit this, the system must have netrom ro CAP_NET_ADMIN capability.
CVE-2023-33203	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/net/ethernet/qualcomm/en unplugs an emac based device.
CVE-2023-33460	There's a memory leak in yajl 2.1.0 with use of yajl_tree_parse function. which will cause out-of-memory in server
CVE-2023-33953	gRPC contains a vulnerability that allows hpack table accounting errors could lead to unwanted disconnects betwee ¬†Three vectors were found that allow the following DOS attacks: - Unbounded memory buffering in the HPACK the HPACK parser The unbounded CPU consumption is down to a copy that occurred per-input-block in the parser to the memory copy bug we end up with an O(n^2) parsing loop, with n selected by the client. The unbounded mem check was behind the string reading code, so we needed to first buffer up to a 4 gigabyte string before rejecting it a have an encoding quirk whereby an infinite number of 0,Äôs can be added at the start of an integer. gRPC,Äôs hpa concluding a parse. - gRPC,Äôs metadata overflow check was performed per frame, so that the following sequence HEADERS: containing a: 1 CONTINUATION: containing a: 2 CONTINUATION: containing a: 3 etc,Ä¶
CVE-2023-3397	A race condition occurred between the functions lmLogClose and txEnd in JFS, in the Linux Kernel, executed in d attacker with normal user privileges to crash the system or leak internal kernel information.
CVE-2023-34256	An issue was discovered in the Linux kernel before 6.3.3. There is an out-of-bounds read in crc16 in lib/crc16.c wh ext4_group_desc_csum does not properly check an offset. NOTE: this is disputed by third parties because the kern with the stated "When modifying the block device while it is mounted by the filesystem" access.
CVE-2023-3567	A use-after-free flaw was found in vcs_read in drivers/tty/vt/vc_screen.c in vc_screen in the Linux Kernel. This iss access to cause a system crash or leak internal kernel information.
CVE-2023-35823	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in saa7134_finidev in drivers
CVE-2023-35824	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in dm1105_remove in drivers
CVE-2023-35828	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in renesas_usb3_remove in d
CVE-2023-35829	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in rkvdec_remove in drivers/
CVE-2023-37453	An issue was discovered in the USB subsystem in the Linux kernel through 6.4.2. There is an out-of-bounds and cr sysfs.c.
CVE-2023-3772	A flaw was found in the Linux kernel,Äôs IP framework for transforming packets (XFRM subsystem). This issue r CAP_NET_ADMIN privileges to directly dereference a NULL pointer in xfrm_update_ae_params(), leading to a p
CVE-2023-3773	A flaw was found in the Linux kernel,Äôs IP framework for transforming packets (XFRM subsystem). This issue r CAP_NET_ADMIN privileges to cause a 4 byte out-of-bounds read of XFRMA_MTIMER_THRESH when parsin leakage of sensitive heap data to userspace.

CVE-2023-3777	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local nf_tables_delrule() is flushing table rules, it is not checked whether the chain is bound and the chain's owner rule c circumstances. We recommend upgrading past commit 6eaf41e87a223ae6f8e7a28d6e78384ad7e407f8.
CVE-2023-37788	goproxy v1.1 was discovered to contain an issue which can lead to a Denial of service (DoS) via unspecified vecto
CVE-2023-38546	This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of c In its API, an application creates 'easy handles' that are the individual handles for single transfers. libcurl provides called curl_easy_duphandle. If a transfer has cookies enabled when the handle is duplicated, the cookie-enable stat actual cookies. If the source handle did not read any cookies from a specific file on disk, the cloned version of the as none (using the four ASCII letters, no quotes).Subsequent use of the cloned handle that does not explicitly set a inadvertently load cookies from a file named none - if such a file exists and is readable in the current directory of t correct file format of course.
CVE-2023-39189	A flaw was found in the Netfilter subsystem in the Linux kernel. The nfnl_osf_add_callback function did not valid This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a cra
CVE-2023-39192	A flaw was found in the Netfilter subsystem in the Linux kernel. The xt_u32 module did not validate the fields in t local privileged attacker to trigger an out-of-bounds read by setting the size fields with a value beyond the array bo disclosure.
CVE-2023-39193	A flaw was found in the Netfilter subsystem in the Linux kernel. The sctp_mt_check did not validate the flag_coun (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a crash or information disclosure.
CVE-2023-39194	A flaw was found in the XFRM subsystem in the Linux kernel. The specific flaw exists within the processing of sta the end of an allocated buffer. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-o information disclosure.
CVE-2023-39197	An out-of-bounds read vulnerability was found in Netfilter Connection Tracking (conntrack) in the Linux kernel. T sensitive information via the DCCP protocol.
CVE-2023-39417	IN THE EXTENSION SCRIPT, a SQL Injection vulnerability was found in PostgreSQL if it uses @extowner@, @ quoting construct (dollar quoting, ", or ""). If an administrator has installed files of a vulnerable, trusted, non-bundl CREATE privilege can execute arbitrary code as the bootstrap superuser.
CVE-2023-40577	Alertmanager handles alerts sent by client applications such as the Prometheus server. An attacker with the permiss alerts endpoint could be able to execute arbitrary JavaScript code on the users of Prometheus Alertmanager. This is 0.2.51.
CVE-2023-4206	A use-after-free vulnerability in the Linux kernel's net/sched: cls_route component can be exploited to achieve loca is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This ca to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the deleted, leading to a use-after-free. We recommend upgrading past commit b80b829e9e2c1b3f7aae34855e04d8f6e
CVE-2023-4207	A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local p called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This caus to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the deleted, leading to a use-after-free. We recommend upgrading past commit 76e42ae831991c828cffa8c37736ebfb8
CVE-2023-4208	A use-after-free vulnerability in the Linux kernel's net/sched: cls_u32 component can be exploited to achieve local called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This caus to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the deleted, leading to a use-after-free. We recommend upgrading past commit 3044b16e7c6fe5d24b1cdbcf1bd0a9d92
CVE-2023-42753	An array indexing vulnerability was found in the netfilter subsystem of the Linux kernel. A missing macro could le offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. Th system or potentially escalate their privileges on the system.
CVE-2023-42754	A NULL pointer dereference flaw was found in the Linux kernel ipv4 stack. The socket buffer (skb) was assumed __ip_options_compile, which is not always the case if the skb is re-routed by ipvs. This issue may allow a local use crash the system.
CVE-2023-42755	A flaw was found in the IPv4 Resource Reservation Protocol (RSVP) classifier in the Linux kernel. The xprt pointe leading to an out-of-bounds read in the `rsvp_classify` function. This issue may allow a local user to crash the syste
CVE-2023-42756	A flaw was found in the Netfilter subsystem of the Linux kernel. A race condition between IPSET_CMD_ADD an panic due to the invocation of `__ip_set_put` on a wrong `set`. This issue may allow a local user to crash the syster
CVE-2023-43785	A vulnerability was found in libX11 due to a boundary condition within the _XkbReadKeySyms() function. This fl bounds read error and read the contents of memory on the system.
CVE-2023-43786	A vulnerability was found in libX11 due to an infinite loop within the PutSubImage() function. This flaw allows a resources and cause a denial of service condition.

CVE-2023-43787	A vulnerability was found in libX11 due to an integer overflow within the XCreateImage() function. This flaw allo and execute arbitrary code with elevated privileges.
CVE-2023-44981	Authorization Bypass Through User-Controlled Key vulnerability in Apache ZooKeeper. If SASL Quorum Peer au (quorum.auth.enableSasl=true), the authorization is done by verifying that the instance part in SASL authentication The instance part in SASL auth ID is optional and if it's missing, like 'eve@EXAMPLE.COM', the authorization ch arbitrary endpoint could join the cluster and begin propagating counterfeit changes to the leader, essentially giving tree.¬†Quorum Peer authentication is not enabled by default.Users are recommended to upgrade to version 3.9.1, 3 ensure the ensemble election/quorum communication is protected by a firewall as this will mitigate the issue.See th cluster administration.
CVE-2023-4569	A memory leak flaw was found in nft_set_catchall_flush in net/netfilter/nf_tables_api.c in the Linux Kernel. This i double-deactivations of catchall elements, which can result in a memory leak.
CVE-2023-45862	An issue was discovered in drivers/usb/storage/ene_ub6250.c for the ENE UB6250 reader driver in the Linux kern extend beyond the end of an allocation.
CVE-2023-45871	An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel before 6. frames larger than the MTU.
CVE-2023-46120	The RabbitMQ Java client library allows Java and JVM-based applications to connect to and interact with RabbitM when receiving Message objects. Attackers could send a very large Message causing a memory overflow and trigg may suffer from DoS attacks from RabbitMQ Java client which will ultimately exhaust the memory of the consum 5.18.0.
CVE-2023-46218	This flaw allows a malicious HTTP server to set "super cookies" in curl that are then passed back to more origins th This allows a site to set cookies that then would get sent to different and unrelated sites and domains. It could do th function that verifies a given cookie domain against the Public Suffix List (PSL). For example a cookie could be se lower case hostname `curl.co.uk`, even though `co.uk` is listed as a PSL domain.
CVE-2023-4622	A use-after-free vulnerability in the Linux kernel's af_unix component can be exploited to achieve local privilege e function tries to add data to the last skb in the peer's recv queue without locking the queue. Thus there is a race whe could access an skb locklessly that is being released by garbage collection, resulting in use-after-free. We recomme 790c2f9d15b594350ae9bca7b236f2b1859de02c.
CVE-2023-4623	A use-after-free vulnerability in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component can escalation. If a class with a link-sharing curve (i.e. with the HFSC_FSC flag set) has a parent without a link-sharing on the parent, but vttree_remove() will be skipped in update_vf(). This leaves a dangling pointer that can cause a us commit b3d26c5702c7d6c45456326e56d2ccf3f103e60f.
CVE-2023-46343	In the Linux kernel before 6.5.9, there is a NULL pointer dereference in send_acknowledge in net/nfc/nci/spi.c.
CVE-2023-4921	A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local used as a class of the qfq qdisc, sending network packets triggers use-after-free in qfq_dequeue() due to the incorre checking in agg_dequeue(). We recommend upgrading past commit 8fc134fee27f2263988ae38920bc03da416b03d
CVE-2023-49295	quic-go is an implementation of the QUIC protocol (RFC 9000, RFC 9001, RFC 9002) in Go. An attacker can caus large number of PATH_CHALLENGE frames. The receiver is supposed to respond to each PATH_CHALLENGE The attacker can prevent the receiver from sending out (the vast majority of) these PATH_RESPONSE frames by c selectively acknowledging received packets) and by manipulating the peer's RTT estimate. This vulnerability has b 0.39.4.
CVE-2023-49568	A denial of service (DoS) vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows a attacks by providing specially crafted responses from a Git server which triggers resource exhaustion in go-git¬†cl filesystem supported by go-git¬†are not affected by this vulnerability. This is a go-git¬†implementation issue and
CVE-2023-49569	A path traversal vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacke filesystem. In the worse case scenario, remote code execution could be achieved. Applications are only affected if t pkg.go.dev/github.com/go-git/go-billy/v5/osfs#ChrootOS , which is the default when using "Plain" versions of Ope Applications using BoundOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#BoundOS ¬†or in-memory file a go-git¬†implementation issue and does not affect the upstream git¬†cli.
CVE-2023-5043	Ingress nginx annotation injection causes arbitrary command execution.
CVE-2023-5044	Code injection via nginx.ingress.kubernetes.io/permanent-redirect annotation.
CVE-2023-51042	In the Linux kernel before 6.4.12, amdgpu_cs_wait_all_fences in drivers/gpu/drm/amd/amdgpu/amdgpu_cs.c has a
CVE-2023-51043	In the Linux kernel before 6.4.5, drivers/gpu/drm/drm_atomic.c has a use-after-free during a race condition betwee unload.

CVE-2023-52438	In the Linux kernel, the following vulnerability has been resolved: binder: fix use-after-free in shinker's callback Tl the shrinker's callback, which means that using alloc->vma pointer isn't safe as it can race with munmap(). As of co zap pages with read mmap_sem in munmap") the mmap lock is downgraded after the vma has been isolated. I was manually adding some delays and triggering page reclaiming through the shrinker's debug sysfs. The following KA ========== BUG: KASAN: slab- +0x470/0x4b8 Read of size 8 at addr ffff356ed50e50f0 by task bash/478 CPU: 1 PID: 478 Comm: bash Not tainted #70 Hardware name: linux,dummy-virt (DT) Call trace: zap_page_range_single+0x470/0x4b8 binder_alloc_free_p +0x130/0x3b0 list_lru_walk_node+0xc4/0x22c binder_shrink_scan+0x108/0x1dc shrinker_debugfs_scan_write+0 vfs_write+0x1ac/0x758 ksys_write+0xf0/0x1dc __arm64_sys_write+0x6c/0x9c Allocated by task 492: kmem_cac +0x2c/0x190 mmap_region+0x258/0x18bc do_mmap+0x694/0xa60 vm_mmap_pgoff+0x170/0x29c ksys_mmap_ +0xcc/0x144 Freed by task 491: kmem_cache_free+0x17c/0x3c8 vm_area_free_rcu_cb+0x74/0x98 rcu_core+0xa3 __do_softirq+0x2fc/0xd24 Last potentially related work creation: __call_rcu_common.constprop.0+0x6c/0xba0 ca remove_vma+0xe4/0x118 do_vmi_align_munmap.isra.0+0x718/0xb5c do_vmi_munmap+0xdc/0x1fc __vm_munm +0x58/0x7c Fix this issue by performing instead a vma_lookup() which will fail to find the vma that was isolated b that this option has better performance than upgrading to a mmap write lock which would increase contention. Plus removed anyway.
CVE-2023-52439	In the Linux kernel, the following vulnerability has been resolved: uio: Fix use-after-free in uio_open core-1 core-2 ---------- uio_unregister_device uio_open idev = idr_find() device_unregister(>dev) uio_device_release get_device(&idev->dev) kfree(idev) uio_free_minor(minor) uio_release put_device(&ide ---------- In the core-1 uio_unregister_device(), the device_unregister will kfre But after core-1 device_unregister, put_device and before doing kfree, the core-2 may get_device. Then: 1. After co free for idev. 2. When core-2 do uio_release and put_device, the idev will be double freed. To address this issue, w with minor_lock.
CVE-2023-52456	In the Linux kernel, the following vulnerability has been resolved: serial: imx: fix tx statemachine deadlock When t tx statemachine is used to control the RTS pin to drive the RS485 transceiver TX_EN pin. When the TTY port is cl (for instance during userland application crash), imx_uart_shutdown disables the interface and disables the Transm imx_uart_stop_tx bails on an incomplete transmission, to be retriggered by the TC interrupt. This interrupt is disab transitions out of SEND. The statemachine is in deadlock now, and the TX_EN remains low, making the interface u incomplete transmission AND whether TC interrupts are enabled before bailing to be retriggered. This makes sure properly set to WAIT_AFTER_SEND.
CVE-2023-52462	In the Linux kernel, the following vulnerability has been resolved: bpf: fix check for attempt to corrupt spilled poin a 1/2/4-byte register, we set slot_type[BPF_REG_SIZE - 1] (plus potentially few more below it, depending on actu has spilled register we need to consult slot_type[7], not slot_type[0]. To avoid the need to remember and double-ch helper.
CVE-2023-52467	In the Linux kernel, the following vulnerability has been resolved: mfd: syscon: Fix null pointer dereference in of_ to dynamically allocated memory which can be NULL upon failure.
CVE-2023-52477	In the Linux kernel, the following vulnerability has been resolved: usb: hub: Guard against accesses to uninitialized usb/core/hub.c and drivers/usb/core/hub.h access fields inside udev->bos without checking if it was allocated and i for whatever reason, udev->bos will be NULL and those accesses will result in a crash: BUG: kernel NULL pointe PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 5 PID: 17818 Comm: kworker/5:1 Tainted: G W 5.1 <HASH:1f9e 1> Hardware name: Google Kindred/Kindred, BIOS Google_Kindred.12672.413.0 02/03/2021 Work 0010:hub_port_reset+0x193/0x788 Code: 89 f7 e8 20 f7 15 00 48 8b 43 08 80 b8 96 03 00 00 03 75 36 0f b7 88 92 a8 03 00 00 <48> 83 78 18 00 74 19 48 89 df 48 8b 75 b0 ba 02 00 00 00 4c 89 e9 RSP: 0018:ffffab740c53fcf8 EF RBX: ffffa1bc5f678000 RCX: 0000000000000310 RDX: ffffffffffffdff RSI: 0000000000000286 RDI: ffffa1be96 00001b7d5edaa20c R09: ffffffffb005e060 R10: 0000000000000001 R11: 0000000000000000 R12: 000000000000 0000000000000032 R15: 0000000000000000 FS: 0000000000000000(0000) GS:ffffa1be96540000(0000) knlGS:0 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000018 CR3: 000000022e80c005 CR4: 00000000003706e0 hub_activate+0x5b7/0x68f process_one_work+0x1a2/0x487 worker_thread+0x11a/0x288 kthread+0x13a/0x152 ? kthread_associate_blkcg+0x70/0x70 ret_from_fork+0x1f/0x30 Fall back to a default behavior if the BOS descripto functionalities that depend on it: LPM support checks, Super Speed capabilitiy checks, U1/U2 states setup.
CVE-2023-52480	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix race condition between session looku ksmbd_session_lookup | smb2_sess_setup sess = xa_load | | | xa_erase(&conn->sessions, sess->id); | | ksmbd_sessi sess->last_active = jiffies | + This patch add rwsem to fix race condition between ksmbd_session_lookup and ksmb

CVE-2023-52484	In the Linux kernel, the following vulnerability has been resolved: iommu/arm-smmu-v3: Fix soft lockup triggered When running an SVA case, the following soft lockup is triggered: ---------- - CPU#244 stuck for 26s! pstate: 83400009 (Nzcv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : arm_smm lr : arm_smmu_cmdq_issue_cmdlist+0x150/0xa50 sp : ffff8000d83ef290 x29: ffff8000d83ef290 x28: 000000003b x26: ffff8000d83ef3c0 x25: da86c0812194a0e8 x24: 0000000000000000 x23: 0000000000000040 x22: ffff8000d8 x20: 0000000000000001 x19: ffff0000c6398080 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000 x14: ffff3000b4a30888 x13: ffff3000b4a3cf60 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000 0000000000000000 x7 : 0000000000000000 x6 : 0000000000048cfa x5 : 0000000000000000 x4 : 0000000000000 0000000080000000 x1 : 0000000000000000 x0 : 0000000000000001 Call trace: arm_smmu_cmdq_issue_cmdlist +0x118/0x254 arm_smmu_tlb_inv_range_asid+0x6c/0x130 arm_smmu_mm_invalidate_range+0xa0/0xa4 __mmu +0x88/0x120 unmap_vmas+0x194/0x1e0 unmap_region+0xb4/0x144 do_mas_align_munmap+0x290/0x490 do_m +0xa8/0x19c __arm64_sys_munmap+0x28/0x50 invoke_syscall+0x78/0x11c el0_svc_common.constprop.0+0x58 +0x2c/0xd4 el0t_64_sync_handler+0x114/0x140 el0t_64_sync+0x1a4/0x1a8 ---------- rc1 the arm_smmu_mm_invalidate_range above is renamed to "arm_smmu_mm_arch_invalidate_secondary_tlbs", 06ff87bae8d3 ("arm64: mm: remove unused functions and variable protoypes") fixed a similar lockup on the CPU too, since arm_smmu_mm_arch_invalidate_secondary_tlbs() is called typically next to MMU tlb flush function, e.g { __flush_tlb_range { // check MAX_TLBI_OPS } } mmu_notifier_arch_invalidate_secondary_tlbs { arm_smmu_ not check MAX_TLBI_OPS } } } Clone a CMDQ_MAX_TLBI_OPS from the MAX_TLBI_OPS in tlbflush.h, sin page table, so it makes sense to align with the tlbflush code. Then, replace per-page TLBI commands with a single hits this threshold.
CVE-2023-52494	In the Linux kernel, the following vulnerability has been resolved: bus: mhi: host: Add alignment check for event r event ring read pointer by "is_valid_ring_ptr" to make sure it is in the buffer range, but there is another risk the poi expecting event ring elements are 128 bits(struct mhi_ring_element) aligned, an unaligned read pointer could lead t memory corruption. So add a alignment check for event ring read pointer.
CVE-2023-52502	In the Linux kernel, the following vulnerability has been resolved: net: nfc: fix races in nfc_llcp_sock_get() and nfc race in nfc_llcp_sock_get(), leading to UAF. Getting a reference on the socket found in a lookup while holding a lo nfc_llcp_sock_get_sn() has a similar problem. Finally nfc_llcp_recv_snl() needs to make sure the socket found by
CVE-2023-52503	In the Linux kernel, the following vulnerability has been resolved: tee: amdtee: fix use-after-free vulnerability in am condition in amdtee_close_session that may cause use-after-free in amdtee_open_session. For instance, if a session free this session via: kref_put(&sess->refcount, destroy_session); the reference count will get decremented, and the However, if in another thread, amdtee_open_session() is called before destroy_session() has completed execution, freed up later in destroy_session() leading to use-after-free in amdtee_open_session. To fix this issue, treat decreme from session list in destroy_session() as a critical section, so that it is executed atomically.
CVE-2023-52507	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: assert requested protocol is valid The p the protocol is supported. Assert the provided protocol is less than the maximum defined so it doesn't potentially pe clearer error for undefined protocols vs unsupported ones.
CVE-2023-52509	In the Linux kernel, the following vulnerability has been resolved: ravb: Fix use-after-free issue in ravb_tx_timeou call cancel_work_sync(). Otherwise, ravb_tx_timeout_work() is possible to use the freed priv after ravb_remove() ravb_tx_timeout() ravb_remove() unregister_netdev() free_netdev(ndev) // free priv ravb_tx_timeout_work() // use so that ravb_stop() is called. And, after phy_stop() is called, netif_carrier_off() is also called. So that .ndo_tx_timeo
CVE-2023-52510	In the Linux kernel, the following vulnerability has been resolved: ieee802154: ca8210: Fix a potential UAF in ca8 ca8210_register_ext_clock(), it calls clk_unregister() to release priv->clk and returns an error. However, the caller where priv->clk is freed again in ca8210_unregister_ext_clock(). In this case, a use-after-free may happen in the se by removing the first clk_unregister(). Also, priv->clk could be an error code on failure of clk_register_fixed_rate(in ca8210_unregister_ext_clock().
CVE-2023-52513	In the Linux kernel, the following vulnerability has been resolved: RDMA/siw: Fix connection failure handling In the newly created endpoint unlinks the listening endpoint and is ready to be dropped. This special case was not han TCP socket close, causing a NULL dereference crash in siw_cm_work_handler() when dereferencing a NULL liste timeout, if immediate MPA request processing fails. This patch furthermore simplifies MPA processing in general: sk_data_ready() upcall is now surpressed, if the socket is already moved out of TCP_ESTABLISHED state.
CVE-2023-52524	In the Linux kernel, the following vulnerability has been resolved: net: nfc: llcp: Add lock when modifying device held when modifying it, or the list could become corrupted, as syzbot discovered.
CVE-2023-52525	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: Fix oob check condition in mwifi path trying to access the rfc1042 headers when the buffer is too small, so the driver can still process packets withou

CVE-2023-52527	In the Linux kernel, the following vulnerability has been resolved: ipv4, ipv6: Fix handling of transhdrlen in __ip{, transhdrlen in length is a problem when the packet is partially filled (e.g. something like send(MSG_MORE) happe to an IPv4 or IPv6 packet as we don't want to repeat the transport header or account for it twice. This can happen u splicing into an L2TP socket. The symptom observed is a warning in __ip6_append_data(): WARNING: CPU: 1 P __ip6_append_data.isra.0+0x1be8/0x47f0 net/ipv6/ip6_output.c:1800 that occurs when MSG_SPLICE_PAGES is partially occupied skbuff. The warning occurs when 'copy' is larger than the amount of data in the message iterator includes the transport header length when it shouldn't. This can be triggered by, for example: sfd = socket(AF_INE bind(sfd, ...); // ::1 connect(sfd, ...); // ::1 port 7 send(sfd, buffer, 4100, MSG_MORE); sendfile(sfd, dfd, NULL, 10 into the length if the write queue is empty in l2tp_ip6_sendmsg(), analogously to how UDP does things. l2tp_ip_se problem as it builds the UDP packet itself.
CVE-2023-52528	In the Linux kernel, the following vulnerability has been resolved: net: usb: smsc75xx: Fix uninit-value access in _ the following uninit-value access issue: ========== in smsc75xx_wait_ready drivers/net/usb/smsc75xx.c:975 [inline] BUG: KMSAN: uninit-value in smsc75xx_bind+ smsc75xx.c:1482 CPU: 0 PID: 8696 Comm: kworker/0:3 Not tainted 5.8.0-rc5-syzkaller #0 Hardware name: Goog Compute Engine, BIOS Google 01/01/2011 Workqueue: usb_hub_wq hub_event Call Trace: __dump_stack lib/du +0x21c/0x280 lib/dump_stack.c:118 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:121 __msan_warning+ smsc75xx_wait_ready drivers/net/usb/smsc75xx.c:975 [inline] smsc75xx_bind+0x5c9/0x11e0 drivers/net/usb/sms drivers/net/usb/usbnet.c:1737 usb_probe_interface+0xece/0x1550 drivers/usb/core/driver.c:374 really_probe+0xf2 driver_probe_device+0x293/0x390 drivers/base/dd.c:701 __device_attach_driver+0x63f/0x830 drivers/base/dd.c:8 base/bus.c:431 __device_attach+0x4e2/0x7f0 drivers/base/dd.c:873 device_initial_probe+0x4a/0x60 drivers/base/c drivers/base/bus.c:491 device_add+0x3b0e/0x40d0 drivers/base/core.c:2680 usb_set_configuration+0x380f/0x3f1 usb_generic_driver_probe+0x138/0x300 drivers/usb/core/generic.c:241 usb_probe_device+0x311/0x490 drivers/u +0xf20/0x20b0 drivers/base/dd.c:529 driver_probe_device+0x293/0x390 drivers/base/dd.c:701 __device_attach_d bus_for_each_drv+0x2ca/0x3f0 drivers/base/bus.c:431 __device_attach+0x4e2/0x7f0 drivers/base/dd.c:873 device dd.c:920 bus_probe_device+0x177/0x3d0 drivers/base/bus.c:491 device_add+0x3b0e/0x40d0 drivers/base/core.c:2 drivers/usb/core/hub.c:2554 hub_port_connect drivers/usb/core/hub.c:5208 [inline] hub_port_connect_change driv drivers/usb/core/hub.c:5494 [inline] hub_event+0x5e7b/0x8a70 drivers/usb/core/hub.c:5576 process_one_work+0x worker_thread+0x10bc/0x2730 kernel/workqueue.c:2415 kthread+0x551/0x590 kernel/kthread.c:292 ret_from_for Local variable ----buf.i87@smsc75xx_bind created at: __smsc75xx_read_reg drivers/net/usb/smsc75xx.c:83 [inlin smsc75xx.c:968 [inline] smsc75xx_bind+0x485/0x11e0 drivers/net/usb/smsc75xx.c:1482 __smsc75xx_read_reg d smsc75xx_wait_ready drivers/net/usb/smsc75xx.c:968 [inline] smsc75xx_bind+0x485/0x11e0 drivers/net/usb/sms usbnet_read_cmd() reads less bytes than requested (zero byte in the reproducer). In this case, 'buf' is not properly fi ENODATA if usbnet_read_cmd() reads less bytes than requested.
CVE-2023-52564	In the Linux kernel, the following vulnerability has been resolved: Revert "tty: n_gsm: fix UAF in gsm_cleanup_m 9b9c8195f3f0d74a826077fc1c01b9ee74907239. The commit above is reverted as it did not solve the original issue virtual ttys by calling gsm_dlci_release() for each available DLCI. There, dlci_put() is called to decrease the refere which finally calls gsm_dlci_free(). This already clears the pointer which is being checked in gsm_cleanup_mux() it is not necessary to clear this pointer in gsm_cleanup_mux() as done in the reverted commit. The commit introduc __die+0x1f/0x70 ? page_fault_oops+0x156/0x420 ? search_exception_tables+0x37/0x50 ? fixup_exception+0x21 asm_exc_page_fault+0x26/0x30 ? tty_port_put+0x19/0xa0 gsmtty_cleanup+0x29/0x80 [n_gsm] release_one_tty+ worker_thread+0x4c/0x3d0 ? __pfx_worker_thread+0x10/0x10 kthread+0xe1/0x110 ? __pfx_kthread+0x10/0x10 +0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK> The actual issue is that nothing guards dlci_put() from bein was triggered but did not yet finished calling gsm_dlci_free().
CVE-2023-52566	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix potential use after free in nilfs_gccach nilfs_gccache_submit_read_data(), brelse(bh) is called to drop the reference count of bh when the call to nilfs_dat_ 0 and its owner page gets unlocked, bh may be freed. However, bh->b_page is dereferenced to put the page after th This patch moves the release operation after unlocking and putting the page. NOTE: The function in question is on current userland tools, address translation using DAT does not occur in that function, so the code path that causes t possible to run that code path by intentionally modifying the userland GC library or by calling the GC ioctl directly to the commit log]
CVE-2023-52567	In the Linux kernel, the following vulnerability has been resolved: serial: 8250_port: Check IRQ data before use In (irq = 0) and IIR register shows that an interrupt happened in the 8250 hardware the IRQ data can be NULL. In suc came to this path from the timer interrupt and quite likely system is already awake. Without this fix we have got an base_baud = 115200) is a 16550A ... BUG: kernel NULL pointer dereference, address: 0000000000000010 RIP: 0 Trace: ? serial8250_handle_irq+0x7c/0x240 ? __pfx_serial8250_timeout+0x10/0x10
CVE-2023-52573	In the Linux kernel, the following vulnerability has been resolved: net: rds: Fix possible NULL-pointer dereference check, if conn pointer exists before dereferencing it as rdma_set_service_type() argument Found by Linux Verifica

CVE-2023-52574	In the Linux kernel, the following vulnerability has been resolved: team: fix null-ptr-deref when team device type i with reproducer [1]. BUG: kernel NULL pointer dereference, address: 0000000000000228 ... RIP: 0010:vlan_dev_ Trace: <TASK> ? __die+0x24/0x70 ? page_fault_oops+0x82/0x150 ? exc_page_fault+0x69/0x150 ? asm_exc_pag +0x35/0x140 [8021q] ? vlan_dev_hard_header+0x8e/0x140 [8021q] neigh_connected_output+0xb2/0x100 ip6_fin +0x43/0xc0 ? ip6_mtu+0x46/0x80 ip6_finish_output+0x2a/0xb0 mld_sendpack+0x18f/0x250 mld_ifc_work+0x39 worker_thread+0x4d/0x2f0 ? __pfx_worker_thread+0x10/0x10 kthread+0xe5/0x120 ? __pfx_kthread+0x10/0x10 +0x10/0x10 ret_from_fork_asm+0x1b/0x30 [1] $ teamd -t team0 -d -c '{"runner": {"name": "loadbalance"}}' $ ip add link t-dummy name t-dummy.100 type vlan id 100 $ ip link add name t-nlmon type nlmon $ ip link set t-nlmon $ ip link set t-dummy up $ ip link set team0 up $ ip link set t-dummy.100 down $ ip link set t-dummy.100 master t device and team device type is changed from non-ether to ether, header_ops of team device is changed to vlan_hea null-ptr-deref for vlan->real_dev in vlan_dev_hard_header() because team device is not a vlan device. Cache eth_h cached header_ops to header_ops of team net device when its type is changed from non-ether to ether to fix the bug
CVE-2023-52577	In the Linux kernel, the following vulnerability has been resolved: dccp: fix dccp_v4_err()/dccp_v6_err() again dh "struct dccp_hdr", not in the "byte 7" as Jann claimed. We need to make sure the ICMP messages are big enough, u assumptions). syzbot reported: BUG: KMSAN: uninit-value in pskb_may_pull_reason include/linux/skbuff.h:2667 pskb_may_pull include/linux/skbuff.h:2681 [inline] BUG: KMSAN: uninit-value in dccp_v6_err+0x426/0x1aa0 n include/linux/skbuff.h:2667 [inline] pskb_may_pull include/linux/skbuff.h:2681 [inline] dccp_v6_err+0x426/0x1a +0x4c7/0x880 net/ipv6/icmp.c:867 icmpv6_rcv+0x19d5/0x30d0 ip6_protocol_deliver_rcu+0xda6/0x2a60 net/ipv6 ip6_input.c:483 [inline] NF_HOOK include/linux/netfilter.h:304 [inline] ip6_input+0x15d/0x430 net/ipv6/ip6_inp ipv6/ip6_input.c:586 dst_input include/net/dst.h:468 [inline] ip6_rcv_finish+0x5db/0x870 net/ipv6/ip6_input.c:79 [inline] ipv6_rcv+0xda/0x390 net/ipv6/ip6_input.c:310 __netif_receive_skb_one_core net/core/dev.c:5523 [inline] core/dev.c:5637 netif_receive_skb_internal net/core/dev.c:5723 [inline] netif_receive_skb+0x58/0x660 net/core/de tun_get_user+0x564c/0x6940 drivers/net/tun.c:2002 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2048 call_w new_sync_write fs/read_write.c:491 [inline] vfs_write+0x8ef/0x15c0 fs/read_write.c:584 ksys_write+0x20f/0x4c0 fs/read_write.c:649 [inline] __se_sys_write fs/read_write.c:646 [inline] __x64_sys_write+0x93/0xd0 fs/read_write common.c:50 [inline] do_syscall_64+0x41/0xc0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwfram slab_post_alloc_hook+0x12f/0xb70 mm/slab.h:767 slab_alloc_node mm/slub.c:3478 [inline] kmem_cache_alloc_ kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:559 __alloc_skb+0x318/0x740 net/core/skbuff.c:650 alloc_skb in alloc_skb_with_frags+0xc8/0xbd0 net/core/skbuff.c:6313 sock_alloc_send_pskb+0xa80/0xbf0 net/core/sock.c:279 [inline] tun_get_user+0x23cf/0x6940 drivers/net/tun.c:1846 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:204 [inline] new_sync_write fs/read_write.c:491 [inline] vfs_write+0x8ef/0x15c0 fs/read_write.c:584 ksys_write+0x20 fs/read_write.c:649 [inline] __se_sys_write fs/read_write.c:646 [inline] __x64_sys_write+0x93/0xd0 fs/read_write common.c:50 [inline] do_syscall_64+0x41/0xc0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwfram syz-executor153 Not tainted 6.6.0-rc1-syzkaller-00014-ga747acc0b752 #0 Hardware name: Google Google Compu Google 08/04/2023
CVE-2023-52578	In the Linux kernel, the following vulnerability has been resolved: net: bridge: use DEV_STATS_INC() syzbot/KC br_handle_frame_finish() [1] This function can run from multiple cpus without mutual exclusion. Adopt SMP safe >stats fields. Handles updates to dev->stats.tx_dropped while we are at it. [1] BUG: KCSAN: data-race in br_hand read-write to 0xffff8881374b2178 of 8 bytes by interrupt on cpu 1: br_handle_frame_finish+0xd4f/0xef0 net/bridg +0x1ed/0x220 br_nf_pre_routing_finish_ipv6+0x50f/0x540 NF_HOOK include/linux/netfilter.h:304 [inline] br_nf bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing+0x526/0xba0 net/bridge/br_netfilter_hooks.c:508 nf_hook_entry [inline] nf_hook_bridge_pre net/bridge/br_input.c:272 [inline] br_handle_frame+0x4c9/0x940 net/bridge/br_input. +0xa8a/0x21e0 net/core/dev.c:5417 __netif_receive_skb_one_core net/core/dev.c:5521 [inline] __netif_receive_sk process_backlog+0x21f/0x380 net/core/dev.c:5965 __napi_poll+0x60/0x3b0 net/core/dev.c:6527 napi_poll net/cor +0x32b/0x750 net/core/dev.c:6727 __do_softirq+0xc1/0x265 kernel/softirq.c:553 run_ksoftirqd+0x17/0x20 kernel +0x30a/0x4a0 kernel/smpboot.c:164 kthread+0x1d7/0x210 kernel/kthread.c:388 ret_from_fork+0x48/0x60 arch/x8 +0x11/0x20 arch/x86/entry/entry_64.S:304 read-write to 0xffff8881374b2178 of 8 bytes by interrupt on cpu 0: br_ net/bridge/br_input.c:189 br_nf_hook_thresh+0x1ed/0x220 br_nf_pre_routing_finish_ipv6+0x50f/0x540 NF_HOO [inline] br_nf_pre_routing_ipv6+0x1e3/0x2a0 net/bridge/br_netfilter_ipv6.c:178 br_nf_pre_routing+0x526/0xba0 nf_hook_entry_hookfn include/linux/netfilter.h:144 [inline] nf_hook_bridge_pre net/bridge/br_input.c:272 [inline] br_input.c:417 __netif_receive_skb_core+0xa8a/0x21e0 net/core/dev.c:5417 __netif_receive_skb_one_core net/co +0x57/0x1b0 net/core/dev.c:5637 process_backlog+0x21f/0x380 net/core/dev.c:5965 __napi_poll+0x60/0x3b0 net dev.c:6594 [inline] net_rx_action+0x32b/0x750 net/core/dev.c:6727 __do_softirq+0xc1/0x265 kernel/softirq.c:553 __local_bh_enable_ip+0x64/0x70 kernel/softirq.c:381 __raw_spin_unlock_bh include/linux/spinlock_api_smp.h:1 +0x36/0x40 kernel/locking/spinlock.c:210 spin_unlock_bh include/linux/spinlock.h:396 [inline] batadv_tt_local_p translation-table.c:1356 batadv_tt_purge+0x2b/0x630 net/batman-adv/translation-table.c:3560 process_one_work process_scheduled_works+0x5b8/0xa30 kernel/workqueue.c:2703 worker_thread+0x525/0x730 kernel/workqueue kthread.c:388 ret_from_fork+0x48/0x60 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x11/0x20 arch/x86/e 0x00000000000d7190 -> 0x00000000000d7191 Reported by Kernel Concurrency Sanitizer on: CPU: 0 PID: 1484 rc1-syzkaller-00236-gad8a69f361b9 #0

CVE-2023-52608	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Check mailbox/SMT chan completion interrupt the shared memory area is accessed to retrieve the message header at first and then, if the mes which is still pending, the related payload is fetched too. When an SCMI command times out the channel ownershi a late reply is received and, as a consequence, any further transmission attempt remains pending, waiting for the ch Once that late reply is received the channel ownership is given back to the agent and any pending request is then al area of the just delivered late reply; then the wait for the reply to the new request starts. It has been observed that th can be wrongly associated with the freshly enqueued request: when that happens the SCMI stack in-flight lookup p message header now present in the SMT area is related to the new pending transaction, even though the real reply h the A2P channel can be detected by looking at the channel status bits: a genuine reply from the platform will have s completion IRQ. Add a consistency check to validate such condition in the A2P ISR.
CVE-2023-52628	In the Linux kernel, the following vulnerability has been resolved: netfilter: nftables: exthdr: fix 4-byte stack OOB dst[len / 4] can write past the destination array which leads to stack corruption. This construct is necessary to clean NOT a multiple of the register size, so make it conditional just like nft_payload.c does. The bug was added in 4.1 c and ip option support was added. Bug reported by Zero Day Initiative project (ZDI-CAN-21950, ZDI-CAN-21951,
CVE-2023-52654	In the Linux kernel, the following vulnerability has been resolved: io_uring/af_unix: disable sending io_uring over lots of problems for io_uring in the past, and it still doesn't work exactly right and races with unix_stream_read_ge disallow sending io_uring files via sockets via SCM_RIGHT, so there are no possible cycles invloving registered f the io_uring side unnecessary.
CVE-2023-52655	In the Linux kernel, the following vulnerability has been resolved: usb: aqc111: check packet for fixup for true lim 0 and sizeof(u64) the value passed to skb_trim() as length will wrap around ending up as some very large value. Th located at that position, which will either oops or process some random value. The fix is to check against sizeof(u6 does. The issue exists since the introduction of the driver.
CVE-2023-52670	In the Linux kernel, the following vulnerability has been resolved: rpmsg: virtio: Free driver_override when rpmsg when rpmsg_remove(), otherwise the following memory leak will occur: unreferenced object 0xffff0000d55d7080 pid 56, jiffies 4294893188 (age 214.272s) hex dump (first 32 bytes): 72 70 6d 73 67 5f 6e 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<000000009c94c9c1>] __kmem_cache_alloc_node+0x1f8 __kmalloc_node_track_caller+0x44/0x70 [<00000000228a60c3>] kstrndup+0x4c/0x90 [<0000000077158695>] d [<000000003e9c4ea5>] rpmsg_register_device_override+0x98/0x170 [<000000001c0c89a8>] rpmsg_ns_register_ rpmsg_probe+0x2e0/0x3ec [<00000000e65a68df>] virtio_dev_probe+0x1c0/0x280 [<00000000443331cc>] really __driver_probe_device+0x78/0xe0 [<00000000a41c9a5b>] driver_probe_device+0xd8/0x160 [<000000009c3bd5 [<0000000043cd7614>] bus_for_each_drv+0x7c/0xd4 [<000000003b929a36>] __device_attach+0x9c/0x19c [<00 +0x14/0x20 [<000000003c999637>] bus_probe_device+0xa0/0xac
CVE-2023-52672	In the Linux kernel, the following vulnerability has been resolved: pipe: wakeup wr_wait after setting max_usage C notification queue support") a regression was introduced that would lock up resized pipes under certain conditions. resizing the pipe ring size was moved to a different function, doing that moved the wakeup for pipe->wr_wait befo pipe was full before the resize occured it would result in the wakeup never actually triggering pipe_write. Set @ma writers if this isn't a watch queue. [Christian Brauner <brauner@kernel.org>: rewrite to account for watch queues]
CVE-2023-52675	In the Linux kernel, the following vulnerability has been resolved: powerpc/imc-pmu: Add a null pointer check in u a pointer to dynamically allocated memory which can be NULL upon failure.
CVE-2023-52677	In the Linux kernel, the following vulnerability has been resolved: riscv: Check if the code to patch lies in the exit s vmalloc_to_page() which panics since the address does not lie in the vmalloc region.
CVE-2023-52682	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to wait on block writeback for post_rea not encrypted, it missed to call f2fs_wait_on_block_writeback() to wait for GCed page writeback in IPU write path - do_garbage_collect - gc_data_segment - move_data_block - f2fs_submit_page_write migrate normal cluster's blo f2fs_write_single_data_page - f2fs_do_write_data_page - f2fs_inplace_write_data - f2fs_submit_page_bio IRQ - f data due to out-of-order GC and common IO. - f2fs_read_end_io
CVE-2023-52686	In the Linux kernel, the following vulnerability has been resolved: powerpc/powernv: Add a null pointer check in c to dynamically allocated memory which can be NULL upon failure.
CVE-2023-52690	In the Linux kernel, the following vulnerability has been resolved: powerpc/powernv: Add a null pointer check to s pointer to dynamically allocated memory which can be NULL upon failure. Add a null pointer check, and release '
CVE-2023-52691	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fix a double-free in si_dpm_init V >pm.dpm.dyn_state.vddc_dependency_on_dispclk.entries fails, amdgpu_free_extended_power_table is called to fr control flow returns to si_dpm_sw_init, it goes to label dpm_failed and calls si_dpm_fini, which calls amdgpu_free fields again. Thus a double-free is triggered.
CVE-2023-52693	In the Linux kernel, the following vulnerability has been resolved: ACPI: video: check for error while searching fo called in acpi_video_dev_register_backlight() fails, for example, because acpi_ut_acquire_mutex() fails inside acpi (uninitialized) acpi_parent handle being passed to acpi_get_pci_dev() for detecting the parent pci device. Check ac only in case of success. Found by Linux Verification Center (linuxtesting.org) with SVACE.

CVE-2023-52694	In the Linux kernel, the following vulnerability has been resolved: drm/bridge: tpd12s015: Drop buggy __exit anno tpd12s015_remove() marked with __exit this function is discarded when the driver is compiled as a built-in. The re no cleanup done which results in resource leakage or worse.
CVE-2023-52696	In the Linux kernel, the following vulnerability has been resolved: powerpc/powernv: Add a null pointer check in c pointer to dynamically allocated memory which can be NULL upon failure.
CVE-2023-52703	In the Linux kernel, the following vulnerability has been resolved: net/usb: kalmia: Don't pass act_len in usb_bulk_ kalmia_send_init_packet() is uninitialized when passing it to the first usb_bulk_msg error path. Jiri Pirko noted tha that the value that would be printed in the second error path would be the value of act_len from the first call to usb_ pass act_len to the usb_bulk_msg error paths. 1: https://lore.kernel.org/lkml/Y9pY61y1nwTuzMOa@nanopsycho/
CVE-2023-52705	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix underflow in second superblock posit NILFS_SB2_OFFSET_BYTES, which computes the position of the second superblock, underflows when the argu Therefore, when using this macro, it is necessary to check in advance that the device size is not less than a lower li occur. The current nilfs2 implementation lacks this check, causing out-of-bound block access when mounting devic loop0, sector 36028797018963960 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 2 NILFS (loop0): unable to rea In addition, when trying to resize the filesystem to a size below 4096 bytes, this underflow occurs in nilfs_resize_fs to nilfs_sufile_resize(), corrupting parameters such as the number of segments in superblocks. This causes excessiv during a subsequent resize ioctl, causing semaphore ns_segctor_sem to block for a long time and hang the writer th more than 143 seconds. Not tainted 6.2.0-rc8-syzkaller-00015-gf6feea56f66d #0 "echo 0 > /proc/sys/kernel/hung_t task:segctord state:D stack:23456 pid:5067 ppid:2 flags:0x00004000 Call Trace: <TASK> context_switch kernel/s +0x1409/0x43f0 kernel/sched/core.c:6606 schedule+0xc3/0x190 kernel/sched/core.c:6682 rwsem_down_write_slo rwsem.c:1190 nilfs_transaction_lock+0x25c/0x4f0 fs/nilfs2/segment.c:357 nilfs_segctor_thread_construct fs/nilfs2 +0x52f/0x1140 fs/nilfs2/segment.c:2570 kthread+0x270/0x300 kernel/kthread.c:376 ret_from_fork+0x1f/0x30 arc Call Trace: <TASK> folio_mark_accessed+0x51c/0xf00 mm/swap.c:515 __nilfs_get_page_block fs/nilfs2/page.c: fs/nilfs2/page.c:61 nilfs_mdt_submit_block+0xd7/0x8f0 fs/nilfs2/mdt.c:121 nilfs_mdt_read_block+0xeb/0x430 fs/ +0x12d/0xbb0 fs/nilfs2/mdt.c:251 nilfs_sufile_get_segment_usage_block fs/nilfs2/sufile.c:92 [inline] nilfs_sufile_ nilfs_sufile_resize+0x7a3/0x12b0 fs/nilfs2/sufile.c:777 nilfs_resize_fs+0x20c/0xed0 fs/nilfs2/super.c:422 nilfs_ioc nilfs_ioctl+0x137c/0x2440 fs/nilfs2/ioctl.c:1301 ... This fixes these issues by inserting appropriate minimum devic depending on where the macro is used.
CVE-2023-52708	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_spi: fix error handling in mmc_spi_ doesn't need to call mmc_remove_host(), or it will cause null-ptr-deref, because of deleting a not added device in m 'fail_glue_init', if mmc_add_host() fails, and change the label 'fail_add_host' to 'fail_gpiod_request'.
CVE-2023-52733	In the Linux kernel, the following vulnerability has been resolved: s390/decompressor: specify __decompress() buf to __decompress() didn't specify "out_len" parameter on many architectures including s390, expecting that no write performed. This has changed since commit 2aa14b1ab2c4 ("zstd: import usptream v1.5.2") which includes zstd libr of dctx by reutilizing dst buffer (#2751)"). Now zstd decompression code might store literal buffer in the unwritten "out_len" is not set, it is considered to be unlimited and hence free to use for optimization needs. On s390 this migh placed right after the decompressor buffer. Luckily the size of uncompressed kernel image is already known to the specify it in the "out_len" parameter.
CVE-2023-52742	In the Linux kernel, the following vulnerability has been resolved: net: USB: Fix wrong-direction WARNING in pl the plusb network driver: A zero-length control-OUT transfer was treated as a read instead of a write. In modern ke usb 1-1: BOGUS control dir, pipe 80000280 doesn't match bRequestType c0 WARNING: CPU: 0 PID: 4645 at dri +0x14a7/0x1880 drivers/usb/core/urb.c:411 Modules linked in: CPU: 1 PID: 4645 Comm: dhcpcd Not tainted 6.2.0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/12/2023 RIP: 0010:u usb/core/urb.c:411 ... Call Trace: <TASK> usb_start_wait_urb+0x101/0x4b0 drivers/usb/core/message.c:58 usb_in message.c:102 [inline] usb_control_msg+0x320/0x4a0 drivers/usb/core/message.c:153 __usbnet_read_cmd+0xb9/ usbnet_read_cmd+0x96/0xf0 drivers/net/usb/usbnet.c:2068 pl_vendor_req drivers/net/usb/plusb.c:60 [inline] pl_se plusb.c:75 [inline] pl_reset+0x2f/0xf0 drivers/net/usb/plusb.c:85 usbnet_open+0xcc/0x5d0 drivers/net/usb/usbnet.c dev.c:1417 __dev_change_flags+0x587/0x750 net/core/dev.c:8530 dev_change_flags+0x97/0x170 net/core/dev.c:8 devinet.c:1147 inet_ioctl+0x33f/0x380 net/ipv4/af_inet.c:979 sock_do_ioctl+0xcc/0x230 net/socket.c:1169 sock_io fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:870 [inline] __se_sys_ioctl fs/ioctl.c:856 [inline] __x64_sys_ioctl+0x arch/x86/entry/common.c:50 [inline] do_syscall_64+0x39/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64 usbnet_write_cmd() instead of usbnet_read_cmd() and remove the USB_DIR_IN flag.
CVE-2023-52746	In the Linux kernel, the following vulnerability has been resolved: xfrm/compat: prevent potential spectre v1 gadge nla_type(nla); if (type > XFRMA_MAX) { return -EOPNOTSUPP; } @type is then used as an array index and can (nla_len(nla) < compat_policy[type].len) { array_index_nospec() can be used to prevent leaking content of kernel m
CVE-2023-52752	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix use-after-free bug in cifs_debug_ that are being teared down (e.g. @ses->ses_status == SES_EXITING) in cifs_debug_data_proc_show() to avoid us following GPF when reading from /proc/fs/cifs/DebugData while mounting and umounting [816.251274] general p canonical address 0x6b6b6b6b6b6b6d81: 0000 [#1] PREEMPT SMP NOPTI ... [816.260138] Call Trace: [816.26 die_addr+0x36/0x90 [816.260762] ? exc_general_protection+0x1b3/0x410 [816.261126] ? asm_exc_general_pro cifs_debug_tcon+0xbd/0x240 [cifs] [816.261878] ? cifs_debug_tcon+0xab/0x240 [cifs] [816.262249] cifs_debug [816.262689] ? seq_read_iter+0x379/0x470 [816.262995] seq_read_iter+0x118/0x470 [816.263291] proc_reg_re srso_alias_return_thunk+0x5/0x7f [816.263945] vfs_read+0x201/0x350 [816.264211] ksys_read+0x75/0x100 [8 [816.264750] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [816.265135] RIP: 0033:0x7fd5e669d381

CVE-2023-52753	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid NULL dereference of t whether assigned timing generator is NULL or not before accessing its funcs to prevent NULL dereference.
CVE-2023-52810	In the Linux kernel, the following vulnerability has been resolved: fs/jfs: Add check for negative db_l2nbperpage l and the minimum legal value should be 0, not negative. In the case of l2nbperpage being negative, an error will occ Syzbot reported this bug: UBSAN: shift-out-of-bounds in fs/jfs/jfs_dmap.c:799:12 shift exponent -16777216 is neg
CVE-2023-52827	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix possible out-of-bound read in a from HTT message and could be an unexpected value in case errors happen, so add validation before using to avoi message iteration and parsing. The same issue also applies to ppdu_info->ppdu_stats.common.num_users, so valid code review. Compile test only.
CVE-2023-52844	In the Linux kernel, the following vulnerability has been resolved: media: vidtv: psi: Add check for kstrdup Add ch return the error if it fails in order to avoid NULL pointer dereference.
CVE-2023-52858	In the Linux kernel, the following vulnerability has been resolved: clk: mediatek: clk-mt7629: Add check for mtk_ value of mtk_alloc_clk_data() in order to avoid NULL pointer dereference.
CVE-2023-52869	In the Linux kernel, the following vulnerability has been resolved: pstore/platform: Add check for kstrdup Add che the error if it fails in order to avoid NULL pointer dereference.
CVE-2023-6176	A null pointer dereference flaw was found in the Linux kernel API for the cryptographic algorithm scatterwalk fun constructs a malicious packet with specific socket configuration, which could allow a local user to crash the system
CVE-2023-6240	A Marvin vulnerability side-channel leakage was found in the RSA decryption operation in the Linux Kernel. This decrypt ciphertexts or forge signatures, limiting the services that use that private key.
CVE-2023-6356	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to s using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver and causing
CVE-2023-6535	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to s using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kern
CVE-2023-6536	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to s using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kern
CVE-2023-6546	A race condition was found in the GSM 0710 tty multiplexor in the Linux kernel. This issue occurs when two threa the same tty file descriptor with the gsm line discipline enabled, and can lead to a use-after-free problem on a struc could allow a local unprivileged user to escalate their privileges on the system.
CVE-2023-6606	An out-of-bounds read vulnerability was found in smbCalcSize in fs/smb/client/netmisc.c in the Linux Kernel. This the system or leak internal kernel information.
CVE-2023-6915	A Null pointer dereference problem was found in ida_free in lib/idr.c in the Linux Kernel. This issue may allow an service problem due to a missing check at a function return.
CVE-2023-6918	A flaw was found in the libssh implements abstract layer for message digest (MD) operations implemented by diffe values from these were not properly checked, which could cause low-memory situations failures, NULL dereferenc memory as an input for the KDF. In this case, non-matching keys will result in decryption/integrity failures, termin
CVE-2023-7192	A memory leak problem was found in ctnetlink_create_conntrack in net/netfilter/nf_conntrack_netlink.c in the Lin attacker with CAP_NET_ADMIN privileges to cause a denial of service (DoS) attack due to a refcount overflow.
CVE-2024-0193	A use-after-free flaw was found in the netfilter subsystem of the Linux kernel. If the catchall element is garbage-co element can be deactivated twice. This can cause a use-after-free issue on an NFT_CHAIN object or NFT_OBJEC with CAP_NET_ADMIN capability to escalate their privileges on the system.
CVE-2024-0775	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allo problem while freeing the old quota file names before a potential failure, leading to a use-after-free.
CVE-2024-21803	Use After Free vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (bluetooth modules) allows Local E associated with program files https://gitee.Com/anolis/cloud-kernel/blob/devel-5.10/net/bluetooth/af_bluetooth.C. T rc2 before v6.8-rc1.
CVE-2024-22189	quic-go is an implementation of the QUIC protocol in Go. Prior to version 0.42.0, an attacker can cause its peer to number of `NEW_CONNECTION_ID` frames that retire old connection IDs. The receiver is supposed to respond `RETIRE_CONNECTION_ID` frame. The attacker can prevent the receiver from sending out (the vast majority of frames by collapsing the peers congestion window (by selectively acknowledging received packets) and by manipu 0.42.0 contains a patch for the issue. No known workarounds are available.
CVE-2024-22257	In Spring Security, versions 5.7.x prior to 5.7.12, 5.8.x prior to 5.8.11, versions 6.0.x prior to 6.0.9, versions 6.1.x p application is possible vulnerable to broken access control when it directly uses the AuthenticatedVoter#vote passi
CVE-2024-22386	A race condition was found in the Linux kernel's drm/exynos device driver in¬†exynos_drm_crtc_atomic_disable(dereference issue, possibly leading to a kernel panic or denial of service issue.

CVE-2024-23342	The `ecdsa` PyPI package is a pure Python implementation of ECC (Elliptic Curve Cryptography) with support for Algorithm), EdDSA (Edwards-curve Digital Signature Algorithm) and ECDH (Elliptic Curve Diffie-Hellman). Ver Minerva attack. As of time of publication, no known patched version exists.
CVE-2024-24864	A race condition was found in the Linux kernel's media/dvb-core in dvbdmx_write()¬†function. This can result in a leading to a kernel panic or denial of service issue.
CVE-2024-26583	In the Linux kernel, the following vulnerability has been resolved: tls: fix race between async notify and socket clo recvmsg/sendmsg) may exit as soon as the async crypto handler calls complete() so any code past that point risks to locking and extra flags altogether. Have the main thread hold an extra reference, this way we can depend solely on Don't futz with reiniting the completion, either, we are now tightly controlling when completion fires.
CVE-2024-26583	In the Linux kernel, the following vulnerability has been resolved: tls: fix race between async notify and socket clo recvmsg/sendmsg) may exit as soon as the async crypto handler calls complete() so any code past that point risks to locking and extra flags altogether. Have the main thread hold an extra reference, this way we can depend solely on Don't futz with reiniting the completion, either, we are now tightly controlling when completion fires.
CVE-2024-26584	In the Linux kernel, the following vulnerability has been resolved: net: tls: handle backlogging of crypto requests S CRYPTO_TFM_REQ_MAY_BACKLOG flag on our requests to the crypto API, crypto_aead_{encrypt,decrypt} c instead of -EINPROGRESS in valid situations. For example, when the cryptd queue for AESNI is full (easy to trig cryptd.cryptd_max_cpu_qlen), requests will be enqueued to the backlog but still processed. In that case, the async c first with err == -EINPROGRESS, which it seems we can just ignore, then with err == 0. Compared to Sabrina's or tls_*crypt_async_wait() helpers and converts the EBUSY to EINPROGRESS to avoid having to modify all the erro
CVE-2024-26585	In the Linux kernel, the following vulnerability has been resolved: tls: fix race between tx work scheduling and soc submitting thread (recvmsg/sendmsg) may exit as soon as the async crypto handler calls complete(). Reorder sched This seems more logical in the first place, as it's the inverse order of what the submitting thread will do.
CVE-2024-26800	In the Linux kernel, the following vulnerability has been resolved: tls: fix use-after-free on failed backlog decryptio to the backlog and crypto_aead_decrypt returns -EBUSY, tls_do_decryption will wait until all async decryptions ha tls_do_decryption will return -EBADMSG and tls_decrypt_sg jumps to the error path, releasing all the pages. But t callback, and have already been released by tls_decrypt_done. The only true async case is when crypto_aead_decry we already waited so we can tell tls_sw_recvmsg that the data is available for immediate copy, but we need to notif flag) that the memory has already been released.
CVE-2024-26811	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate payload size in ipc response If i ksmbd.mountd can return invalid ipc response to ksmbd kernel server. ksmbd should validate payload size of ipc re overrun or slab-out-of-bounds. This patch validate 3 ipc response that has payload.
CVE-2024-26841	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Update cpu_sibling_map when disa cpu_sibling_map when disabling nonboot CPUs by defining & calling clear_cpu_sibling_map(), otherwise we get s label: negative count! WARNING: CPU: 6 PID: 45 at kernel/jump_label.c:263 __static_key_slow_dec_cpuslocked cpuhp/6 Not tainted 6.8.0-rc5+ #1340 pc 90000000004c302c ra 90000000004c302c tp 90000001005bc000 sp 9000 900000000224c278 a2 90000001005bfb58 a3 900000000224c280 a4 900000000224c278 a5 90000001005bfb50 a t0 ce87a4763eb5234a t1 ce87a4763eb5234a t2 0000000000000000 t3 0000000000000000 t4 0000000000000006 t t7 0000000000001964 t8 000000000009ebf6 u0 9000000001f2a068 s9 0000000000000000 s0 900000000246a2d8 90000000021518c0 s4 0000000000000040 s5 9000000002151058 s6 9000000009828e40 s7 00000000000000b4 s __static_key_slow_dec_cpuslocked+0xec/0x100 ERA: 90000000004c302c __static_key_slow_dec_cpuslocked+0x -IE -DA +PG DACF=CC DACM=CC -WE) PRMD: 00000004 (PPLV0 +PIE -PWE) EUEN: 00000000 (-FPE -SX (LIE=2-4,10-12 VS=7) ESTAT: 000c0000 [BRK] (IS= ECode=12 EsubCode=0) PRID: 0014d000 (Loongson-64b 45 Comm: cpuhp/6 Not tainted 6.8.0-rc5+ #1340 Stack : 0000000000000000 900000000203f258 900000000179af 0000000000000000 90000001005bf988 9000000001fe0be0 900000000224c280 900000000224c278 90000001005 0000000000000001 ce87a4763eb5234a 0000000007f38000 90000001003f8cc0 0000000000000000 00000000000 4c206e6f73676e6f 6f4c203a656d616e 000000000009ec99 0000000007f38000 0000000000000000 900000000214 0000000000000000 0000000000000107 0000000000000009 ffffffffffafdabe 00000000000000b4 00000000000000 00005555939a0c7c 00000000000000b0 0000000000000004 0000000000000000 0000000000071c1c ... Call Trace +0x48/0x1a0 [<900000000179afc8>] dump_stack_lvl+0x78/0xa0 [<9000000000263ed0>] __warn+0x90/0x1a0 [< +0x1b8/0x280 [<900000000179c564>] do_bp+0x264/0x420 [<90000000004c302c>] __static_key_slow_dec_cpus sched_cpu_deactivate+0x2fc/0x300 [<9000000000266498>] cpuhp_invoke_callback+0x178/0x8a0 [<900000000 [<90000000002a117c>] smpboot_thread_fn+0x1dc/0x2e0 [<900000000029a720>] kthread+0x140/0x160 [<90000 +0xc/0xa4

CVE-2024-26893	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Fix double free in SMC tra code tears down a channel, it calls the chan_free callback function, defined by each transport. Since multiple protoc member, chan_free() might want to clean up the same member multiple times within the given SCMI transport imp transport. This will lead to a NULL pointer dereference at the second time: | scmi_protocol scmi_dev.1: Enabled po | arm-scmi firmware:scmi: SCMI Notifications - Core Enabled. | arm-scmi firmware:scmi: unable to communicate NULL pointer dereference at virtual address 0000000000000000 | Mem abort info: | ESR = 0x0000000096000004 32 bits | SET = 0, FnV = 0 | EA = 0, S1PTW = 0 | FSC = 0x04: level 0 translation fault | Data abort info: | ISV = 0, | CM = 0, WnR = 0, TnD = 0, TagAccess = 0 | GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 | user pgtable: 4k pages, [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 | Internal error: Oops: 000000009600000 | CPU: 4 PID: 1 Comm: swapper/0 Not tainted 6.7.0-rc2-00124-g455ef3d016c9-dirty #793 | Hardware name: FVP daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) | pc : smc_chan_free+0x3c/0x6c | lr : smc_chan_free+0x3c/0x6c | idr_for_each+0x68/0xf8 | scmi_cleanup_channels.isra.0+0x2c/0x58 | scmi_probe+0x434/0x734 | platform_probe | __driver_probe_device+0x78/0x12c | driver_probe_device+0x3c/0x118 | __driver_attach+0x74/0x128 | bus_for_ +0x24/0x30 | bus_add_driver+0xe4/0x1e8 | driver_register+0x60/0x128 | __platform_driver_register+0x28/0x34 | +0x78/0x33c | kernel_init_freeable+0x2b8/0x51c | kernel_init+0x24/0x130 | ret_from_fork+0x10/0x20 | Code: f00 (b9400280) | ---[end trace 0000000000000000]--- Simply check for the struct pointer being NULL before trying t This was found when a transport doesn't really work (for instance no SMC service), the probe routines then tries to
CVE-2024-26896	In the Linux kernel, the following vulnerability has been resolved: wifi: wfx: fix memory leak when starting AP Kr object 0xd73d1180 (size 184): comm "wpa_supplicant", pid 1559, jiffies 13006305 (age 964.245s) hex dump (first 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 1e 00 01 00 00 00 00 00 ..... backtrace: [<5ca11420>] km __alloc_skb+0x144/0x170 [<fb8a5e38>] __netdev_alloc_skb+0x50/0x180 [<0f9fa1d5>] __ieee80211_beacon_get ieee80211_beacon_get_tim+0x54/0x18c [mac80211] [<41e25cc3>] wfx_start_ap+0xc8/0x234 [wfx] [<93a70356> [mac80211] [<a4a661cd>] nl80211_start_ap+0x76c/0x9e0 [cfg80211] [<47bd8b68>] genl_rcv_msg+0x198/0x378 +0xd0/0x130 [<6b7c977a>] genl_rcv+0x34/0x44 [<66b2d04d>] netlink_unicast+0x1b4/0x258 [<f965b9b6>] netli ____sys_sendmsg+0x1e0/0x274 [<d2b5212d>] ___sys_sendmsg+0x80/0xb4 [<69954f45>] __sys_sendmsg+0x64 (size 1024): comm "wpa_supplicant", pid 1559, jiffies 13006305 (age 964.246s) hex dump (first 32 bytes): 00 00 0 00 00 00 ..... 10 00 07 40 00 00 00 00 00 00 00 00 00 00 00 00 ...@..... backtrace: [<9a993714>] __kma [<f83ea192>] kmalloc_reserve.constprop.0+0x30/0x74 [<a2c61343>] __alloc_skb+0xa0/0x170 [<fb8a5e38>] __n __ieee80211_beacon_get+0x290/0x4d4 [mac80211] [<7accd02d>] ieee80211_beacon_get_tim+0x54/0x18c [mac8 +0xc8/0x234 [wfx] [<93a70356>] ieee80211_start_ap+0x404/0x6b4 [mac80211] [<a4a661cd>] nl80211_start_ap genl_rcv_msg+0x198/0x378 [<453ef796>] netlink_rcv_skb+0xd0/0x130 [<6b7c977a>] genl_rcv+0x34/0x44 [<66 [<f965b9b6>] netlink_sendmsg+0x1e8/0x428 [<aadb8231>] ____sys_sendmsg+0x1e0/0x274 [<d2b5212d>] ___s kernel is build optimized, it seems the stack is not accurate. It appears the issue is related to wfx_set_mfp_ap(). The allocated by ieee80211_beacon_get() is never released. Fixing this leak makes kmemleak happy.
CVE-2024-26907	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix fortify source warning while [cut here]------------ memcpy: detected field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /va build/drivers/infiniband/hw/mlx5/wr.c:131 (size 2) WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx-ofed-k hw/mlx5/wr.c:131 mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] Modules linked in: 8021q garp mrp stp llc rdma_ ib_ipoib(OE) ib_cm(OE) ib_umad(OE) mlx5_ib(OE) ib_uverbs(OE) ib_core(OE) mlx5_core(OE) pci_hyperv_intf mlxfw(OE) psample nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nf nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ip_set nf_tables libcrc32c nfnetlink mst_pciconf(OE) knem(OE) vfio vfio iommufd irqbypass cuse nfsv3 nfs fscache netfs xfrm_user xfrm_algo ipmi_devintf ipmi_msghandler binfmt_ polyval_clmulni polyval_generic ghash_clmulni_intel sha512_ssse3 snd_pcsp aesni_intel crypto_simd cryptd snd_ input_leds serio_raw evbug nfsd auth_rpcgss nfs_acl lockd grace sch_fq_codel sunrpc drm efi_pstore ip_tables x_t net_failover failover floppy [last unloaded: mlx_compat(OE)] CPU: 0 PID: 293779 Comm: ssh Tainted: G OE 6.2. Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011 RIP: 0010:mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] a0 b9 02 00 00 00 48 c7 c2 10 5b fd c0 48 c7 c7 80 5b fd c0 c6 05 57 0c 03 00 01 e8 95 4d 93 da <0f> 0b 44 8b 4d ff ff 41 0f b7 RSP: 0018:ffffb5b48478b570 EFLAGS: 00010046 RAX: 0000000000000000 RBX: 0000000000000 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffb5b48478b628 R08: 0000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffb5b48478b5e8 R13: ffff963a3c609b5e R14: ffff9639c FS: 00007fc03b444c80(0000) GS:ffff963a3dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 000 0000556f46bdf000 CR3: 0000000006ac6003 CR4: 0000000003706f0 DR0: 0000000000000000 DR1: 00000000 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? show_regs+0x72/0x [mlx5_ib] ? __warn+0x8d/0x160 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? report_bug+0x1bb/0x1d0 ? ha +0x19/0x80 ? asm_exc_invalid_op+0x1b/0x20 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] mlx5_ib_post_sen +0x2ec/0x770 [ib_ipoib] ipoib_start_xmit+0x5a0/0x770 [ib_ipoib] dev_hard_start_xmit+0x8e/0x1e0 ? validate_xm +0x116/0x3a0 __dev_xmit_skb+0x1fd/0x580 __dev_queue_xmit+0x284/0x6b0 ? _raw_spin_unlock_irq+0xe/0x5 push_pseudo_header+0x17/0x40 [ib_ipoib] neigh_connected_output+0xcd/0x110 ip_finish_output2+0x179/0x480 __ip_finish_output+0xc3/0x190 ip_finish_output+0x2e/0xf0 ip_output+0x78/0x110 ? __pfx_ip_finish_output+0x1 __ip_queue_xmit+0x18a/0x460 ip_queue_xmit+0x15/0x30 __tcp_transmit_skb+0x914/0x9c0 tcp_write_xmit+0x3 tcp_sendmsg_locked+0x2e1/0xac0 tcp_sendmsg+0x2d/0x50 inet_sendmsg+0x43/0x90 sock_sendmsg+0x68/0x80 +0x326/0x3c0 ksys_write+0xbd/0xf0 ? do_syscall_64+0x69/0x90 __x64_sys_write+0x19/0x30 do_syscall_ ---trun
CVE-2024-26913	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix dcn35 8k30 Underflow/C missing for pipe split policy determination and cause Underflow/Corruption issue. [how] Add the odm calculation.
CVE-2024-26914	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix incorrect mpc_combine ar stream, while MAX_PLANES is per asic. The mpc_combine is an array that records all the planes per asic. Therefo array size. Using MAX_SURFACES causes array overflow when there are more than 3 planes. [how] Use the MA

CVE-2024-26952	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix potencial out-of-bounds when buffer bounds when buffer offset fields of a few requests is invalid. This patch set the minimum value of buffer offset fiel
CVE-2024-27034	In the Linux kernel, the following vulnerability has been resolved: f2fs: compress: fix to cover normal cluster write compressed cluster w/ normal cluster, we should not unlock cp_rwsem during f2fs_write_raw_pages(), otherwise d persisted before CP & SPOR, due to cluster metadata wasn't updated atomically.
CVE-2024-27035	In the Linux kernel, the following vulnerability has been resolved: f2fs: compress: fix to guarantee persisting comp compressed cluster is not persisted with metadata during checkpoint, after SPOR, the data may be corrupted, let's g checkpoint.
CVE-2024-27389	In the Linux kernel, the following vulnerability has been resolved: pstore: inode: Only d_invalidate() is needed Unl records in pstorefs would trigger the dput() double-drop warning: WARNING: CPU: 0 PID: 2569 at fs/dcache.c:76 of d_drop()/dput() (as mentioned in Documentation/filesystems/vfs.rst) isn't the right approach here, and leads to th Use d_invalidate() and update the code to not bother checking for error codes that can never happen. ---
CVE-2024-27393	In the Linux kernel, the following vulnerability has been resolved: xen-netfront: Add missing skb_mark_for_recycl introduced later than fixes tag in commit 6a5bcd84e886 ("page_pool: Allow drivers to hint on SKB recycling"). It to page_pool_release_page() between v5.9 to v5.14, after which is should have used skb_mark_for_recycle(). Sinc were removed (in commit 535b9c61bdef ("net: page_pool: hide page_pool_release_page()") and remaining callers branch 'net-page_pool-remove-page_pool_release_page'")). This leak became visible in v6.8 via commit dba1b8a7 memory leaks").
CVE-2024-28849	follow-redirects is an open source, drop-in replacement for Node's `http` and `https` modules that automatically fol follow-redirects only clears authorization header during cross-domain redirect, but keep the proxy-authentication h vulnerability may lead to credentials leak, but has been addressed in version 1.15.6. Users are advised to upgrade. T vulnerability.
CVE-2024-35785	In the Linux kernel, the following vulnerability has been resolved: tee: optee: Fix kernel panic caused by incorrect to register devices on the TEE bus has a bug leading to kernel panic as follows: [15.398930] Unable to handle kern ffff07ed00626d7c [15.406913] Mem abort info: [15.409722] ESR = 0x0000000096000005 [15.413490] EC = 0x [15.418814] SET = 0, FnV = 0 [15.421878] EA = 0, S1PTW = 0 [15.425031] FSC = 0x05: level 1 translation fau ISV = 0, ISS = 0x00000005, ISS2 = 0x00000000 [15.438310] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [15.44 = 0, Xs = 0 [15.448697] swapper pgtable: 4k pages, 48-bit VAs, pgdp=00000000d9e3e000 [15.455413] [ffff07ed p4d=1800000bffdf9003, pud=0000000000000000 [15.464146] Internal error: Oops: 0000000096000005 [#1] PRE optee: Fix supplicant based device enumeration") lead to the introduction of this bug. So fix it appropriately.
CVE-2024-35796	In the Linux kernel, the following vulnerability has been resolved: net: ll_temac: platform_get_resource replaced b platform_get_resource was replaced with devm_platform_ioremap_resource_byname and is called using 0 as name platform_get_resource_byname in the call stack, where it causes a null pointer in strcmp. if (type == resource_type have been replaced with devm_platform_ioremap_resource.
CVE-2024-35811	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: Fix use-after-free bug in brcmf patch of CVE-2023-47233 : https://nvd.nist.gov/vuln/detail/CVE-2023-47233 In brcm80211 driver,it starts with th timeout worker: ->brcmf_usb_probe ->brcmf_usb_probe_cb ->brcmf_attach ->brcmf_bus_started ->brcmf_cfg802 ->INIT_WORK(&cfg->escan_timeout_work, brcmf_cfg80211_escan_timeout_worker); If we disconnect the USB to make cleanup. The invoking chain is : brcmf_usb_disconnect ->brcmf_usb_disconnect_cb ->brcmf_detach ->br the timeout woker may still be running. This will cause a use-after-free bug on cfg in brcmf_cfg80211_escan_time canceling the worker in brcmf_cfg80211_detach. [arend.vanspriel@broadcom.com: keep timer delete as is and can
CVE-2024-35818	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Define the __io_aw() hook as mmi ("drivers: Remove explicit invocations of mmiowb()") remove all mmiowb() in drivers, but it says: "NOTE: mmiow in conjunction with spin_unlock(). However, pairing each mmiowb() removal in this patch with the corresponding so there is a small chance that this change may regress any drivers incorrectly relying on mmiowb() to order MMIO synchronisation." The mmio in radeon_ring_commit() is protected by a mutex rather than a spinlock, but in the mu We can add mmiowb() calls in the radeon driver but the maintainer says he doesn't like such a workaround, and rad protected mmio. So we should extend the mmiowb tracking system from spinlock to mutex, and maybe other locki prone, so we solve it in the architectural code, by simply defining the __io_aw() hook as mmiowb(). And we no lon so use the generic definition. Without this, we get such an error when run 'glxgears' on weak ordering architectures ring 0 stalled for more than 10324msec radeon 0000:04:00.0: ring 3 stalled for more than 10240msec radeon 0000: 0x000000000001f412 last fence id 0x000000000001f414 on ring 3) radeon 0000:04:00.0: GPU lockup (current fen 0x000000000000f941 on ring 0) radeon 0000:04:00.0: scheduling IB failed (-35). [drm:radeon_gem_va_ioctl [rade (-35) radeon 0000:04:00.0: scheduling IB failed (-35). [drm:radeon_gem_va_ioctl [radeon]] *ERROR* Couldn't up scheduling IB failed (-35). [drm:radeon_gem_va_ioctl [radeon]] *ERROR* Couldn't update BO_VA (-35) radeon [drm:radeon_gem_va_ioctl [radeon]] *ERROR* Couldn't update BO_VA (-35) radeon 0000:04:00.0: scheduling IB [radeon]] *ERROR* Couldn't update BO_VA (-35) radeon 0000:04:00.0: scheduling IB failed (-35). [drm:radeon_ update BO_VA (-35) radeon 0000:04:00.0: scheduling IB failed (-35). [drm:radeon_gem_va_ioctl [radeon]] *ERR
CVE-2024-35829	In the Linux kernel, the following vulnerability has been resolved: drm/lima: fix a memleak in lima_heap_alloc Wh need to be deallocated, or there will be memleaks.

CVE-2024-35833	In the Linux kernel, the following vulnerability has been resolved: dmaengine: fsl-qdma: Fix a memory leak relate dma_alloc_coherent() is undone neither in the remove function, nor in the error handling path of fsl_qdma_probe() issues.
CVE-2024-35835	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: fix a double-free in arfs_create_grou arfs_create_groups will free ft->g and return an error. However, arfs_create_table, the only caller of arfs_create_gr mlx5e_destroy_flow_table, in which the ft->g will be freed again.
CVE-2024-35844	In the Linux kernel, the following vulnerability has been resolved: f2fs: compress: fix reserve_cblocks counting err one direct_node, performing the following operations will cause the file to be unrepairable: unisoc # ./f2fs_io comp dev/block/dm-48 112G 112G 1.2M 100% /data unisoc # ./f2fs_io release_cblocks test.apk 924 unisoc # df -h | grep 100% /data unisoc # dd if=/dev/random of=file4 bs=1M count=3 3145728 bytes (3.0 M) copied, 0.025 s, 120 M/s u 112G 112G 1.8M 100% /data unisoc # ./f2fs_io reserve_cblocks test.apk F2FS_IOC_RESERVE_COMPRESS_BL reboot unisoc # df -h | grep dm-48 /dev/block/dm-48 112G 112G 11M 100% /data unisoc # ./f2fs_io reserve_cbloc one direct_node. After returning to -ENOSPC, reserved_blocks += ret will not be executed. As a result, the reserve the real number of reserved blocks. Therefore, fsck cannot be set to repair the file. After this patch, the fsck flag wi grep dm-48 /dev/block/dm-48 112G 112G 1.8M 100% /data unisoc # ./f2fs_io reserve_cblocks test.apk F2FS_IOC No space left on device adb reboot then fsck will be executed unisoc # df -h | grep dm-48 /dev/block/dm-48 112G reserve_cblocks test.apk 924
CVE-2024-35845	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: dbg-tlv: ensure NUL termination string, so we must ensure the string is terminated correctly before using it.
CVE-2024-35879	In the Linux kernel, the following vulnerability has been resolved: of: dynamic: Synchronize of_changeset_destroy sequence: 1) of_platform_depopulate() 2) of_overlay_remove() During the step 1, devices are destroyed and devlin are destroyed but __of_changeset_entry_destroy() can raise warnings related to missing of_node_put(): ERROR: n 2 ... Indeed, during the devlink removals performed at step 1, the removal itself releasing the device (and the attach workqueue and so, it is done asynchronously with respect to function calls. When the warning is present, of_node_ the workqueue job. In order to be sure that any ongoing devlink removals are done before the of_node destruction, the devlink removals.
CVE-2024-35902	In the Linux kernel, the following vulnerability has been resolved: net/rds: fix possible cp null dereference cp migh null dereference [Simon Horman adds:] Analysis: * cp is a parameter of __rds_rdma_map and is not reassigned. * cp argument to __rds_rdma_map() - rds_get_mr() - rds_get_mr_for_dest * Prior to the code above, the following a indicative, but could itself be unnecessary) trans_private = rs->rs_transport->get_mr(sg, nents, rs, &mr->r_key, cp args->vec.bytes, need_odp ? ODP_ZEROBASED : ODP_NOT_NEEDED); * The code modified by this patch is g trans_private is assigned as per the previous point in this analysis. The only implementation of get_mr that I could an ERR_PTR if the conn (4th) argument is NULL. * ret is set to PTR_ERR(trans_private). rds_ib_get_mr can retu argument is NULL. Thus ret may be -ENODEV in which case the code in question will execute. Conclusion: * cp adds a check; this patch does seem to address a possible bug
CVE-2024-35956	In the Linux kernel, the following vulnerability has been resolved: btrfs: qgroup: fix qgroup prealloc rsv leak in sub create snapshot and delete subvolume all use btrfs_subvolume_reserve_metadata() to reserve metadata for the chan tree, which cannot be mediated in the normal way via start_transaction. When quota groups (squota or qgroups) are of type PREALLOC. Once the operation is associated to a transaction, we convert PREALLOC to PERTRANS, wi transaction. However, the error paths of these three operations were not implementing this lifecycle correctly. They to PERTRANS in a generic cleanup step regardless of errors or whether the operation was fully associated to a tran occasionally converting this rsv to PERTRANS without calling record_root_in_trans successfully, which meant tha transaction by some other thread, the end of the transaction would not free that root's PERTRANS, leaking it. Ultim CONFIG_BTRFS_DEBUG builds at unmount for the leaked reservation. The fix is to ensure that every qgroup PR properties: 1. any failure before record_root_in_trans is called successfully results in freeing the PREALLOC reser we convert to PERTRANS, and now the transaction owns freeing the reservation. This patch enforces those proper generic/269 with squotas enabled at mkfs time would fail in ~5-10 runs on my system. With this patch, it ran succe
CVE-2024-35971	In the Linux kernel, the following vulnerability has been resolved: net: ks8851: Handle softirqs at the end of IRQ th thread may call ks8851_rx_pkts() in case there are any packets in the MAC FIFO, which calls netif_rx(). This netif local_bh_disable() and local_bh_enable(). The local_bh_enable() may call do_softirq() to run softirqs in case any a net_rx_action, which ultimately reaches the driver .start_xmit callback. If that happens, the system hangs. The entir from netdev_start_xmit netdev_start_xmit from dev_hard_start_xmit dev_hard_start_xmit from sch_direct_xmit sc __dev_queue_xmit from __neigh_update __neigh_update from neigh_update neigh_update from arp_process.const __netif_receive_skb_one_core __netif_receive_skb_one_core from process_backlog process_backlog from __napi from net_rx_action net_rx_action from __do_softirq __do_softirq from call_with_stack call_with_stack from do_s __local_bh_enable_ip from netif_rx netif_rx from ks8851_irq ks8851_irq from irq_thread_fn irq_thread_fn from ir from ret_from_fork The hang happens because ks8851_irq() first locks a spinlock in ks8851_par.c ks8851_lock_pa with that spinlock locked, calls netif_rx(). Once the execution reaches ks8851_start_xmit_par(), it calls ks8851_loc already locked spinlock again, and the hang happens. Move the do_softirq() call outside of the spinlock protected s around the entire spinlock protected section of ks8851_irq() handler. Place local_bh_enable() outside of the spinloc do_softirq() without the ks8851_par.c ks8851_lock_par() spinlock being held, and safely call ks8851_start_xmit_p locked spinlock. Since ks8851_irq() is protected by local_bh_disable()/local_bh_enable() now, replace netif_rx() w local_bh_disable()/local_bh_enable() calls.

CVE-2024-35988	In the Linux kernel, the following vulnerability has been resolved: riscv: Fix TASK_SIZE on 64-bit NOMMU On anywhere in physical RAM. The current definition of TASK_SIZE is wrong if any RAM exists above 4G, causing routines.
CVE-2024-35990	In the Linux kernel, the following vulnerability has been resolved: dma: xilinx_dpdma: Fix locking There are sever chan->vchan.lock was not held. Add appropriate locking. This fixes lockdep warnings like [31.077578] ---------- WARNING: CPU: 2 PID: 40 at drivers/dma/xilinx/xilinx_dpdma.c:834 xilinx_dpdma_chan_queue_transfer+0x27 linked in: [31.078019] CPU: 2 PID: 40 Comm: kworker/u12:1 Not tainted 6.6.20+ #98 [31.078102] Hardware nar Workqueue: events_unbound deferred_probe_work_func [31.078272] pstate: 600000c5 (nZCv daIF -PAN -UAO [31.078377] pc : xilinx_dpdma_chan_queue_transfer+0x274/0x5e0 [31.078473] lr : xilinx_dpdma_chan_queue_t sp : ffffffc083bb2e10 [31.078590] x29: ffffffc083bb2e10 x28: 0000000000000000 x27: ffffff880165a168 [31.078 ffffff880164eab8 x24: ffffff880164d480 [31.078920] x23: ffffff880165a148 x22: ffffff880164e988 x21: 0000000 ffffffc082aa3000 x19: ffffff880164e880 x18: 0000000000000000 [31.079295] x17: 0000000000000000 x16: 0000 [31.079453] x14: 0000000000000000 x13: ffffff8802263dc0 x12: 0000000000000001 [31.079613] x11: 0001ffc0 x9 : 0001ffc082aa3def [31.079824] x8 : 0001ffc082aa3dec x7 : 0000000000000000 x6 : 0000000000000516 [31. ffffff88003c9c40 x3 : ffffffffffffffff [31.080147] x2 : ffffffc7f8d43000 x1 : 00000000000000c0 x0 : 0000000000 xilinx_dpdma_chan_queue_transfer+0x274/0x5e0 [31.080518] xilinx_dpdma_issue_pending+0x11c/0x120 [31.0 +0x180/0x3ac [31.080712] zynqmp_dpsub_plane_atomic_update+0x11c/0x21c [31.080825] drm_atomic_helper_ drm_atomic_helper_commit_tail+0x5c/0xb0 [31.081139] commit_tail+0x234/0x294 [31.081246] drm_atomic_he drm_atomic_commit+0x100/0x140 [31.081477] drm_client_modeset_commit_atomic+0x318/0x384 [31.081634] +0x8c/0x24c [31.081725] drm_client_modeset_commit+0x34/0x5c [31.081812] __drm_fb_helper_restore_fbdev [31.081899] drm_fb_helper_set_par+0x50/0x70 [31.081971] fbcon_init+0x538/0xc48 [31.082047] visual_init+0 do_bind_con_driver.isra.0+0x2d0/0x634 [31.082320] do_take_over_console+0x24c/0x33c [31.082429] do_fbcon fbcon_fb_registered+0x2d0/0x34c [31.082663] register_framebuffer+0x27c/0x38c [31.082767] __drm_fb_helper [31.082939] drm_fb_helper_initial_config+0x50/0x74 [31.083012] drm_fbdev_dma_client_hotplug+0xb8/0x108 +0xa0/0xf4 [31.083195] drm_fbdev_dma_setup+0xb0/0x1cc [31.083293] zynqmp_dpsub_drm_init+0x45c/0x4e0 +0x444/0x5e0 [31.083616] platform_probe+0x8c/0x13c [31.083713] really_probe+0x258/0x59c [31.083793] __ [31.083878] driver_probe_device+0x70/0x1c0 [31.083961] __device_attach_driver+0x108/0x1e0 [31.084052] b [31.084125] __device_attach+0x100/0x298 [31.084207] device_initial_probe+0x14/0x20 [31.084292] bus_probe deferred_probe_work_func+0x11c/0x180 [31.084451] process_one_work+0x3ac/0x988 [31.084643] worker_thre +0x1bc/0x1c0 [31.084848] ret_from_fork+0x10/0x20 [31.084932] irq event stamp: 64549 [31.084970] hardirqs _raw_spin_unlock_irqrestore+0x80/0x90 [31.085157] ---truncated---
CVE-2024-36008	In the Linux kernel, the following vulnerability has been resolved: ipv4: check for NULL idev in ip_route_use_hin deref in fib_validate_source() in an old tree [1]. It appears the bug exists in latest trees. All calls to __in_dev_get_r result. [1] general protection fault, probably for non-canonical address 0xdfffc0000000000: 0000 [#1] SMP KASA [0x0000000000000000-0x0000000000000007] CPU: 2 PID: 3257 Comm: syz-executor.3 Not tainted 5.10.0-syzka (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 RIP: 0010:fib_validate_source+0xbf/0x1 f2 f2 f2 42 c7 44 20 23 f3 f3 f3 f3 48 89 44 24 78 42 c6 44 20 27 f3 e8 5d 88 48 fc 4c 89 e8 48 c1 e8 03 48 89 44 2 15 98 fc 48 89 5c 24 10 41 bf RSP: 0018:ffffc900015fee40 EFLAGS: 00010246 RAX: 0000000000000000 RBX: RDX: 0000000000000000 RSI: 0000000004001eac RDI: ffff8880160c64c0 RBP: ffffc900015ff060 R08: 0000000 R10: 0000000000000002 R11: ffff88800f4f90c0 R12: dfffc0000000000 R13: 0000000000000000 R14: 0000000 FS: 00007f938acfe6c0(0000) GS:ffff888058c00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 000 00007f938acddd58 CR3: 000000001248e000 CR4: 0000000000352ef0 DR0: 0000000000000000 DR1: 0000000 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: ip_route_use_hint+0x410/0x9b +0x2c4/0x1a30 net/ipv4/ip_input.c:327 ip_list_rcv_finish net/ipv4/ip_input.c:612 [inline] ip_sublist_rcv+0x3ed/0x +0x422/0x470 net/ipv4/ip_input.c:673 __netif_receive_skb_list_ptype net/core/dev.c:5572 [inline] __netif_receive dev.c:5620 __netif_receive_skb_list net/core/dev.c:5672 [inline] netif_receive_skb_list_internal+0x9f9/0xdc0 net/ +0x55/0x3e0 net/core/dev.c:5816 xdp_recv_frames net/bpf/test_run.c:257 [inline] xdp_test_run_batch net/bpf/test_ +0x1818/0x1d00 net/bpf/test_run.c:363 bpf_prog_test_run_xdp+0x81f/0x1170 net/bpf/test_run.c:1376 bpf_prog_t syscall.c:3736 __sys_bpf+0x45c/0x710 kernel/bpf/syscall.c:5115 __do_sys_bpf kernel/bpf/syscall.c:5201 [inline] _ [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5199
CVE-2024-36898	In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: fix uninitialised kfifo If a line is r debouncing in software, and the line is subsequently reconfigured to enable edge detection then the allocation of th This results in events being written to and read from an uninitialised kfifo. Read events are returned to userspace. I software debounce is already active.
CVE-2024-36899	In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: Fix use after free in lineinfo_chan as follows: when the GPIO chip device file is being closed by invoking gpio_chrdev_release(), watched_lines is fre of lineinfo_changed_nb notifier chain failed due to waiting write rwsem. Additionally, one of the GPIO chip's lines notifier chain's read rwsem. Consequently, a race condition leads to the use-after-free of watched_lines. Here is the gpio_chrdev_release() --> bitmap_free(cdev->watched_lines) <-- freed --> blocking_notifier_chain_unregister() --> rwsem --> __down_write_common() --> rwsem_down_write_slowpath() --> schedule_preempt_disabled() --> sche gpio_free() --> gpiod_free() --> gpiod_free_commit() --> gpiod_line_state_notify() --> blocking_notifier_call_cha rwsem --> notifier_call_chain() --> lineinfo_changed_notify() --> test_bit(xxxx, cdev->watched_lines) <-- use afte issue is that a GPIO line event is being generated for userspace where it shouldn't. However, since the chrdev is bei read that event anyway. To fix the issue, call the bitmap_free() function after the unregistration of lineinfo_changed

CVE-2024-36942	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: qca: fix firmware check error path A firmware files before downloading them to the controller but introduced a memory leak in case the sanity checks ev before returning on errors.
CVE-2024-36964	In the Linux kernel, the following vulnerability has been resolved: fs/9p: only translate RWX permissions for plain bits is allowed through, which causes it to be able to set (among others) the suid bit. This was presumably not the in explicitly and conditionally on .u.
CVE-2024-38577	In the Linux kernel, the following vulnerability has been resolved: rcu-tasks: Fix show_rcu_tasks_trace_gp_kthread buffer overflow in show_rcu_tasks_trace_gp_kthread() if counters, passed to sprintf() are huge. Counter numbers, n buffer overflow is still possible. Use snprintf() with buffer size instead of sprintf(). Found by Linux Verification Ce
CVE-2024-38620	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: HCI: Remove HCI_AMP support Sin controllers no longer has any use so remove it along with the capability of creating AMP controllers. Since we no l Primary controllers, as only HCI_PRIMARY is left, this also remove hdev->dev_type altogether.
CVE-2024-38667	In the Linux kernel, the following vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary i should be reserved for pt_regs. However this is not the case for the idle threads of the secondary boot harts. Their s may get corrupted. Similar issue has been fixed for the primary hart, see c7cdd96eca28 ("riscv: prevent stack corru However that fix was not propagated to the secondary harts. The problem has been noticed in some CPU hotplug te stored several registers on stack, corrupting top of pt_regs structure including status field. As a result, kernel attemp
CVE-2024-39496	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix use-after-free due to race with c creation of a block group, we can race with a device replace operation and then trigger a use-after-free on the devic the replace operation). This happens because at btrfs_load_zone_info() we extract a device from the chunk map int while not under the protection of the device replace rwsem. So if there's a device replace operation happening when source of the replace operation, we will trigger a use-after-free if before we finish using the device the replace oper enlarging the critical section under the protection of the device replace rwsem so that all uses of the device are done
CVE-2024-39496	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix use-after-free due to race with c creation of a block group, we can race with a device replace operation and then trigger a use-after-free on the devic the replace operation). This happens because at btrfs_load_zone_info() we extract a device from the chunk map int while not under the protection of the device replace rwsem. So if there's a device replace operation happening when source of the replace operation, we will trigger a use-after-free if before we finish using the device the replace oper enlarging the critical section under the protection of the device replace rwsem so that all uses of the device are done
CVE-2024-39497	In the Linux kernel, the following vulnerability has been resolved: drm/shmem-helper: Fix BUG_ON() on mmap(P of check for copy-on-write (COW) mapping in drm_gem_shmem_mmap allows users to call mmap with PROT_W a kernel panic due to BUG_ON in vmf_insert_pfn_prot: BUG_ON((vma->vm_flags & VM_PFNMAP) && is_cow EINVAL early if COW mapping is detected. This bug affects all drm drivers using default shmem helpers. It can b *ptr = mmap(0, size, PROT_WRITE, MAP_PRIVATE, fd, mmap_offset); ptr[0] = 0;
CVE-2024-39507	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash problem in concurren driver need to notify the roce driver to handle this event, but at this time, the roce driver may uninit, then cause ker status change, need to check whether the roce registered, and when uninit, need to wait link update finish.
CVE-2024-39508	In the Linux kernel, the following vulnerability has been resolved: io_uring/io-wq: Use set_bit() and test_bit() at w on worker->flags within io_uring/io-wq to address potential data races. The structure io_worker->flags may be acc to concurrency issues. When KCSAN is enabled, it reveals data races occurring in io_worker_handle_work and io_ BUG: KCSAN: data-race in io_worker_handle_work / io_wq_activate_free_worker write to 0xffff8885c4246404 o io_worker_handle_work (io_uring/io-wq.c:434 io_uring/io-wq.c:569) io_wq_worker (io_uring/io-wq.c:?) <snip> r by task 49024 on cpu 5: io_wq_activate_free_worker (io_uring/io-wq.c:? io_uring/io-wq.c:285) io_wq_enqueue (io (io_uring/io_uring.c:524) io_req_task_submit (io_uring/io_uring.c:1511) io_handle_tw_list (io_uring/io_uring.c:11 18daea77cca6 ("Merge tag 'for-linus' of git://git.kernel.org/pub/scm/virt/kvm/kvm"). These races involve writes an different tasks running on different CPUs. To mitigate this, refactor the code to use atomic operations such as set_b "and" and "or" operations. This ensures thread-safe manipulation of worker flags. Also, move `create_index` to avo

CVE-2024-39510	In the Linux kernel, the following vulnerability has been resolved: cachefiles: fix slab-use-after-free in cachefiles_ondemand_daemon_read() We got the following issue in a fuzz test of randomly issuing the restore com ========== BUG: KASAN: slab- cachefiles_ondemand_daemon_read+0xb41/0xb60 Read of size 8 at addr ffff888122e84088 by task ondemand-04- Comm: ondemand-04-dae Not tainted 6.8.0-dirty #564 Call Trace: kasan_report+0x93/0xc0 cachefiles_ondemand_ vfs_read+0x169/0xb50 ksys_read+0xf5/0x1e0 Allocated by task 116: kmem_cache_alloc+0x140/0x3a0 cachefiles fscache_cookie_state_machine+0x43c/0x1230 [...] Freed by task 792: kmem_cache_free+0xfe/0x390 cachefiles_p fscache_cookie_state_machine+0x5c8/0x1230 [...] ========== Following is the process that triggers the issue: mount | daemon_thread1 | daemon_thread2 ---------- cachefiles_withdraw_cookie cachefiles_ondemand_clean_object(object) cachefiles_ondemand_send_req REQ_A = wait_for_completion(&REQ_A->done) cachefiles_daemon_read cachefiles_ondemand_daemon_read REQ_A = ca msg->object_id = req->object->ondemand->ondemand_id ------ restore ------ cachefiles_ondemand_restore xas_fo xas_set_mark(&xas, CACHEFILES_REQ_NEW) cachefiles_daemon_read cachefiles_ondemand_daemon_read R copy_to_user(_buffer, msg, n) xa_erase(&cache->reqs, id) complete(&REQ_A->done) ------ close(fd) ------ cachef cachefiles_put_object cachefiles_put_object kmem_cache_free(cachefiles_object_jar, object) REQ_A->object->on When we see the request within xa_lock, req->object must not have been freed yet, so grab the reference count of c issue.
CVE-2024-40899	In the Linux kernel, the following vulnerability has been resolved: cachefiles: fix slab-use-after-free in cachefiles_c issue in a fuzz test of randomly issuing the restore command: ========== BUG: KASAN: slab-use-after-free in cachefiles_ondemand_daemon_read+0x609/0xab0 Write of size 4 at addr fff ondemand-04-dae/4962 CPU: 11 PID: 4962 Comm: ondemand-04-dae Not tainted 6.8.0-rc7-dirty #542 Call Trace: cachefiles_ondemand_daemon_read+0x609/0xab0 vfs_read+0x169/0xb50 ksys_read+0xf5/0x1e0 Allocated by tas +0x1df/0x4b0 cachefiles_ondemand_send_req+0x24d/0x690 cachefiles_create_tmpfile+0x249/0xb30 cachefiles_c cachefiles_look_up_object+0x29c/0xa60 cachefiles_lookup_cookie+0x37d/0xca0 fscache_cookie_state_machine+ by task 626: kfree+0xf1/0x2c0 cachefiles_ondemand_send_req+0x568/0x690 cachefiles_create_tmpfile+0x249/0x +0x6f/0x140 cachefiles_look_up_object+0x29c/0xa60 cachefiles_lookup_cookie+0x37d/0xca0 fscache_cookie_st ========== Following is the proc daemon_thread1 | daemon_thread2 ---------- cachefiles_ondemand_init_o REQ_A = kzalloc(sizeof(*req) + data_len) wait_for_completion(&REQ_A->done) cachefiles_daemon_read cache REQ_A = cachefiles_ondemand_select_req cachefiles_ondemand_get_fd copy_to_user(_buffer, msg, n) process_o restore ------ cachefiles_ondemand_restore xas_for_each(&xas, req, ULONG_MAX) xas_set_mark(&xas, CACHE cachefiles_daemon_read cachefiles_ondemand_daemon_read REQ_A = cachefiles_ondemand_select_req write(de size)); cachefiles_ondemand_copen xa_erase(&cache->reqs, id) complete(&REQ_A->done) kfree(REQ_A) cachef get_unused_fd_flags file = anon_inode_getfile fd_install(fd, file) load = (void *)REQ_A->msg.data; load->fd = fd; issuing a restore command when the daemon is still alive, which results in a request being processed multiple times problem, add an additional reference count to cachefiles_req, which is held while waiting and reading, and then rel Note that since there is only one reference count for waiting, we need to avoid the same request being completed m request if it is successfully removed from the xarray.
CVE-2024-40900	In the Linux kernel, the following vulnerability has been resolved: cachefiles: remove requests from xarray during CACHEFILES_DEAD set, we can still read the requests, so in the following concurrency the request may be used daemon_thread1 | daemon_thread2 ---------- cachefiles_ondemand_init_o REQ_A = kzalloc(sizeof(*req) + data_len) wait_for_completion(&REQ_A->done) cachefiles_daemon_read cache dev fd cachefiles_flush_reqs complete(&REQ_A->done) kfree(REQ_A) xa_lock(&cache->reqs); cachefiles_onder CACHEFILES_OP_READ // req use-after-free !!! xa_unlock(&cache->reqs); xa_destroy(&cache->reqs) Hence re flushing them to avoid accessing freed requests.
CVE-2024-40910	In the Linux kernel, the following vulnerability has been resolved: ax25: Fix refcount imbalance on inbound conne ax25_release(), we call netdev_put() to decrease the refcount on the associated ax.25 device. However, the executio never calls netdev_hold(). This imbalance leads to refcount errors, and ultimately to kernel crashes. A typical call t one of the following errors: refcount_t: decrement hit 0; leaking memory. refcount_t: underflow; use-after-free. An <TASK> ? show_regs+0x64/0x70 ? __warn+0x83/0x120 ? refcount_warn_saturate+0xb2/0x100 ? report_bug+0x1 handle_bug+0x3e/0x70 ? exc_invalid_op+0x1c/0x70 ? asm_exc_invalid_op+0x1f/0x30 ? refcount_warn_saturate+ +0xb2/0x100 ax25_release+0x2ad/0x360 __sock_release+0x35/0xa0 sock_close+0x19/0x20 [...] On reboot (or any gets stuck in an infinite loop: unregister_netdevice: waiting for ax0 to become free. Usage count = 0 This patch cor netdev_hold() and ax25_dev_hold() for new connections in ax25_accept(). This makes the logic leading to ax25_a both cases we increment the refcount, which is ultimately decremented in ax25_release().

CVE-2024-40915	In the Linux kernel, the following vulnerability has been resolved: riscv: rewrite __kernel_map_pages() to fix sleep is a debug function which clears the valid bit in page table entry for deallocated pages to detect illegal memory acc set/clear the valid bit using __set_memory(). __set_memory() acquires init_mm's semaphore, and this operation ma __kernel_map_pages() can be called in atomic context, and thus is illegal to sleep. An example warning that this ca invalid context at kernel/locking/rwsem.c:1578 in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 2, name: kthre 0 PID: 2 Comm: kthreadd Not tainted 6.9.0-g1d4c6d784ef6 #37 Hardware name: riscv-virtio,qemu (DT) Call Trac +0x1c/0x24 [<ffffffff8091ef6e>] show_stack+0x2c/0x38 [<ffffffff8092baf8>] dump_stack_lvl+0x5a/0x72 [<ffffff [<ffffffff8003b7ac>] __might_resched+0x104/0x10e [<ffffffff8003b7f4>] __might_sleep+0x3e/0x62 [<ffffffff809 [<ffffffff8000cf00>] __set_memory+0x82/0x2fa [<ffffffff8000d324>] __kernel_map_pages+0x5a/0xd4 [<ffffffff8 [<ffffffff8018ee82>] __vmalloc_node_range+0x196/0x6ba [<ffffffff80011904>] copy_process+0x72c/0x17ec [<ff [<ffffffff80012f62>] kernel_thread+0x82/0xa0 [<ffffffff8003552c>] kthreadd+0x14a/0x1be [<ffffffff809357de>] with apply_to_existing_page_range(). It is fine to not have any locking, because __kernel_map_pages() works with pages are not changed by anyone else in the meantime.
CVE-2024-40918	In the Linux kernel, the following vulnerability has been resolved: parisc: Try to fix random segmentation faults in PA8800 and PA8900 processors have had problems with random segmentation faults for many years. Systems with Systems with PA8800 and PA8900 processors have a large L2 cache which needs per page flushing for decent perf The combined cache in these systems is also more sensitive to non-equivalent aliases than the caches in earlier syst faults that I have looked at appear to be memory corruption in memory allocated using mmap and malloc. My first work. On reviewing the cache code, I realized that there were two issues which the existing code didn't handle corr issue is that the present bit in PTEs is racy. 1) PA-RISC caches have a mind of their own and they can speculatively long as there is a entry in the TLB for the page which allows move-in. TLBs are local to each CPU. Thus, the TLB flushing the page. This is particularly important on SMP systems. In some of the flush routines, the flush routine w would be purged. This was because the flush routine needed the TLB entry to do the flush. 2) My initial approach t try and use flush_cache_page_if_present for all flush operations. This actually made things worse and led to a coup on me that some lines weren't being flushed because the pte check code was racy. This resulted in random inequiva __flush_cache_page tmpalias flush sets up its own TLB entry and it doesn't need the existing TLB entry. As long a we can get the pfn and physical address of the page. We can also purge the TLB entry for the page before doing the special TLB entry that inhibits cache move-in. When switching page mappings, we need to ensure that lines are rer just flush the lines to memory as they may come back. This made it clear that we needed to implement all the requi This includes flushes for user and kernel pages. After modifying the code to use tmpalias flushes, it became clear th fully resolved. The frequency of faults was worse on systems with a 64 MB L2 (PA8900) and systems with more C to flush_cache_page_if_present to detect pages that couldn't be flushed triggered frequently on some systems. Helg flushed and found that the PTE was either cleared or for a swap page. Ignoring pages that were swapped out seeme problematic. I looked at routines related to pte_clear and noticed ptep_clear_flush. The default implementation just obvious that on parisc we need to flush the cache page as well. If we don't flush the cache page, stale lines will be l Once a PTE is cleared, there is no way to find the physical address associated with the PTE and flush the associated updated change with a parisc specific version of ptep_clear_flush. It fixed the random data corruption on Helge's rp this point, I realized that I could restore the code where we only flush in flush_cache_page_if_present if the page h need to flush the cache when the accessed bit is cleared in ---truncated---
CVE-2024-40927	In the Linux kernel, the following vulnerability has been resolved: xhci: Handle TD clearing for multiple streams c multiple TDs might be in flight when an endpoint is stopped. We need to issue a Set TR Dequeue Pointer for each, and the caches cleared. Change the logic so that any N>1 TDs found active for different streams are deferred until a xhci_invalidate_cancelled_tds() again from xhci_handle_cmd_set_deq() to queue another command until we are do error/"should never happen" paths to ensure we at least clear any affected TDs, even if we can't issue a command to loudly with an xhci_warn() if this ever happens. This problem case dates back to commit e9df17eb1408 ("USB: xh rings per endpoint.") early on in the XHCI driver's life, when stream support was first added. It was then identified in commit 674f8438c121 ("xhci: split handling halted endpoints into two steps"), which added a FIXME comment changing the behavior as far as I can tell, though the new logic made the problem more obvious). Then later, in cor give back some cached cancelled URBs."), it was acknowledged again. [Mathias: commit 94f339147fc3 ("xhci: Fix URBs.") was a targeted regression fix to the previously mentioned patch. Users reported issues with usb stuck after This rolled back the TD clearing of multiple streams to its original state.] Apparently the commit author was aware It was still mentioned as a FIXME, an xhci_dbg() was added to log the problem condition, and the remaining issue The choice of making the log type xhci_dbg() for what is, at this point, a completely unhandled and known broken it guarantees that no actual users would see the log in production, thereby making it nigh undebuggable (indeed, ev doesn't really hint at there being a problem at all). It took me *months* of random xHC crashes to finally find a rel debug session, which could all have been avoided had this unhandled, broken condition been actually reported with intentionally left in unfixed (never mind that it shouldn't have been left in at all). > Another fix to solve clearing the TDs is needed, but not as urgent. 3 years after that statement and 14 years after the original bug was introduced, I th next time let's not leave bugs unfixed (that are actually worse than the original bug), and let's actually get people to crashes and IOMMU faults with UAS devices when handling errors/faults. Easiest repro is to use `hdparm` to mark bad, then `cat /dev/sdX > /dev/null` in a loop. At least in the case of JMicron controllers, the read errors end up hav requests to different streams) and the one that didn't get cleared properly ends up faulting the xHC entirely when it been unmapped, referred to by the stale TDs. This normally happens quickly (after two or three loops). After this fi and experienced no xHC failures, with all read errors recovered properly. Repro'd and tested on an Apple M1 Mac IOMMU, this bug would instead silently corrupt freed memory, making this a ---truncated---

CVE-2024-40947	In the Linux kernel, the following vulnerability has been resolved: ima: Avoid blocking in RCU read-side critical s BUG: unable to handle kernel NULL pointer dereference at 0000000000000010 PGD 42f873067 P4D 0 Oops: 000 1286325 Comm: kubeletmonit.sh Kdump: loaded Tainted: P Hardware name: QEMU Standard PC (i440FX + PIIX 0010:ima_match_policy+0x84/0x450 Code: 49 89 fc 41 89 cf 31 ed 89 44 24 14 eb 1c 44 39 7b 18 74 26 41 83 ff 0 9c 01 00 00 <44> 85 73 10 74 ea 44 8b 6b 14 41 f6 c5 01 75 d4 41 f6 c5 02 74 0f RSP: 0018:ff71570009e07a80 E RBX: 0000000000000000 RCX: 0000000000000200 RDX: ffffffffad8dc7c0 RSI: 0000000024924925 RDI: ff3e27 R08: 0000000000000000 R09: ffffffffabfce739 R10: ff3e27810cc42400 R11: 0000000000000000 R12: ff3e27818 000000000000000c R15: 0000000000000001 FS: 00007f5195b51740(0000) GS:ff3e278b12d40000(0000) knlGS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000010 CR3: 0000000626d24002 CR4: 00000000003 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 000000000 +0x22/0x30 process_measurement+0xb0/0x830 ? page_add_file_rmap+0x15/0x170 ? alloc_set_pte+0x269/0x4c0 simple_xattr_get+0x75/0xa0 ? selinux_file_open+0x9d/0xf0 ima_file_check+0x64/0x90 path_openat+0x571/0x17 page_counter_try_charge+0x57/0xc0 ? files_cgroup_alloc_fd+0x38/0x60 ? __alloc_fd+0xd4/0x250 ? do_sys_oper +0x1bd/0x250 do_syscall_64+0x5d/0x1d0 entry_SYSCALL_64_after_hwframe+0x65/0xca Commit c7423dbdbc9 ima_filter_rule_match()") introduced call to ima_lsm_copy_rule within a RCU read-side critical section which con implies a possible sleep and violates limitations of RCU read-side critical sections on non-PREEMPT systems. Sle might cause synchronize_rcu() returning early and break RCU protection, allowing a UAF to happen. The root cau follows: | Thread A | Thread B | |ima_match_policy | | | rcu_read_lock | |ima_lsm_update_rule | | | synchronize_rcu ==> synchronize_rcu returns early | kfree(entry) | | | | entry = entry->next| ==> UAF happens and entry now becom >action | ==> Accessing entry might cause panic. To fix this issue, we are converting all kmalloc that is called with GFP_ATOMIC. [PM: fixed missing comment, long lines, !CONFIG_IMA_LSM_RULES case]
CVE-2024-40953	In the Linux kernel, the following vulnerability has been resolved: KVM: Fix a data race on last_boosted_vcpu in k {READ,WRITE}_ONCE() to access kvm->last_boosted_vcpu to ensure the loads and stores are atomic. In the ext tears the stores, it's theoretically possible for KVM to attempt to get a vCPU using an out-of-bounds index, e.g. if th and is paired with a 32-bit load on a VM with 257 vCPUs: CPU0 CPU1 last_boosted_vcpu = 0xff; (last_boosted_v 0x01; i = (last_boosted_vcpu = 0x1ff) last_boosted_vcpu[7:0] = 0x00; vcpu = kvm->vcpu_array[0x1ff]; As detecte in kvm_vcpu_on_spin [kvm] / kvm_vcpu_on_spin [kvm] write to 0xffffc90025a92344 of 4 bytes by task 4340 on c kvm/../../../virt/kvm/kvm_main.c:4112) kvm handle_pause (arch/x86/kvm/vmx/vmx.c:5929) kvm_intel vmx_handl x86/kvm/vmx/vmx.c:6606) kvm_intel vcpu_run (arch/x86/kvm/x86.c:11107 arch/x86/kvm/x86.c:11211) kvm kvm x86.c:?) kvm kvm_vcpu_ioctl (arch/x86/kvm/../../../virt/kvm/kvm_main.c:?) kvm __se_sys_ioctl (fs/ioctl.c:52 fs/io (fs/ioctl.c:890) x64_sys_call (arch/x86/entry/syscall_64.c:33) do_syscall_64 (arch/x86/entry/common.c:?) entry_S entry/entry_64.S:130) read to 0xffffc90025a92344 of 4 bytes by task 4342 on cpu 4: kvm_vcpu_on_spin (arch/x86 kvm handle_pause (arch/x86/kvm/vmx/vmx.c:5929) kvm_intel vmx_handle_exit (arch/x86/kvm/vmx/vmx.c:? arch vcpu_run (arch/x86/kvm/x86.c:11107 arch/x86/kvm/x86.c:11211) kvm kvm_arch_vcpu_ioctl_run (arch/x86/kvm/x kvm/../../../virt/kvm/kvm_main.c:?) kvm __se_sys_ioctl (fs/ioctl.c:52 fs/ioctl.c:904 fs/ioctl.c:890) __x64_sys_ioctl syscall_64.c:33) do_syscall_64 (arch/x86/entry/common.c:?) entry_SYSCALL_64_after_hwframe (arch/x86/entry -> 0x00000000
CVE-2024-40965	In the Linux kernel, the following vulnerability has been resolved: i2c: lpi2c: Avoid calling clk_get_rate during tra clk_get_rate for each transfer, lock the clock rate and cache the value. A deadlock has been observed while adding When this clock provider adds its clock, the clk mutex is locked already, it needs to access i2c, which in return nee
CVE-2024-40967	In the Linux kernel, the following vulnerability has been resolved: serial: imx: Introduce timeout when waiting on t second for USR2_TXDC to be set, we avoid a potential deadlock. In case of the timeout, there is not much we can and optimistically try to continue.
CVE-2024-40969	In the Linux kernel, the following vulnerability has been resolved: f2fs: don't set RO when shutting down f2fs Shut due to readonly, which causes a deadlock like below. f2fs_ioc_shutdown(F2FS_GOING_DOWN_FULLSYNC) is freeze_super - f2fs_stop_checkpoint() - f2fs_handle_critical_error - sb_start_write - set RO - waiting - bdev_thaw sb_rdonly() - f2fs_stop_discard_thread -> wait for kthread_stop(discard_thread);
CVE-2024-40970	In the Linux kernel, the following vulnerability has been resolved: Avoid hw_desc array overrun in dw-axi-dmac I and in which each descriptor is composed by 3 segments, resulting in the DMA channel descs_allocated to be 9. Si considering the descs_allocated, this scenario would result in a kernel panic (hw_desc array will be overrun). To fi to the axi_dma_desc structure, where we keep the number of allocated hw_descs (axi_desc_alloc()) and use it in ax correctly. Additionally I propose to remove the axi_chan_start_first_queued() call after completing the transfer, sin (started descriptors can be interrupted and transfer ignored due to DMA channel not being enabled).
CVE-2024-40971	In the Linux kernel, the following vulnerability has been resolved: f2fs: remove clear SB_INLINECRYPT flag in c SB_INLINECRYPT flag will be clear and re-set. If create new file or open file during this gap, these files will not lead to data corruption if wrappedkey_v0 is enable. Thread A: Thread B: -f2fs_remount -f2fs_file_open or f2fs_ne SB_INLINECRYPT flag -fscrypt_select_encryption_impl -parse_options <- set SB_INLINECRYPT again
CVE-2024-40973	In the Linux kernel, the following vulnerability has been resolved: media: mtk-vcodec: potential null pointer defere devm_kzalloc() needs to be checked to avoid NULL pointer deference. This is similar to CVE-2022-3113.

CVE-2024-40975	In the Linux kernel, the following vulnerability has been resolved: platform/x86: x86-android-tablets: Unregister d subsystems support a device getting removed while there are still consumers of the device with a reference to the d regulator subsystem. If a regulator gets unregistered while there are still drivers holding a reference a WARN() at d e.g.: WARNING: CPU: 1 PID: 1587 at drivers/regulator/core.c:5829 regulator_unregister Hardware name: Intel Co BYT-T FFD8, BIOS BLADE_21.X64.0005.R00.1504101516 FFD8_X64_R_2015_04_10_1516 04/10/2015 RIP: <TASK> regulator_unregister devres_release_group i2c_device_remove device_release_driver_internal bus_remo x86_android_tablet_remove On the Lenovo Yoga Tablet 2 series the bq24190 charger chip also provides a 5V boo devices connected to the micro USB port, the bq24190-charger driver exports this as a Vbus regulator. On the 830 is controlled by a platform_device and x86_android_tablet_remove() removes platform_device-s before i2c_clients on the 1380 (13") model there is a lc824206xa micro-USB switch connected over I2C and the extcon driver for tha client *must* be registered first, because that creates the regulator with the lc824206xa listed as its consumer. If th lc824206xa driver will end up getting a dummy regulator. Since in this case both the regulator provider and consu that the consumer is unregistered first is to unregister the I2C devices in reverse order of in which they were create problems in the future change x86_android_tablet_remove() to unregister all device types in reverse order.
CVE-2024-40976	In the Linux kernel, the following vulnerability has been resolved: drm/lima: mask irqs in timeout path before hard a rendering job might take just long enough to trigger the drm sched job timeout handler but also still complete bef handler. This runs into race conditions not expected by the timeout handler. In some very specific cases it currently lima_pm_idle, with a stack dump such as: [10136.669170] WARNING: CPU: 0 PID: 0 at drivers/gpu/drm/lima/lim +0xa0/0xb0 ... [10136.669459] pc : lima_devfreq_record_idle+0xa0/0xb0 ... [10136.669628] Call trace: [10136.66 [10136.669646] lima_sched_pipe_task_done+0x5c/0xb0 [10136.669656] lima_gp_irq_handler+0xa8/0x120 [1013 +0x48/0x160 [10136.669679] handle_irq_event+0x4c/0xc0 We can prevent that race condition entirely by maskin handler, at which point we give up on waiting for that job entirely. The irqs will be enabled again at the next hard r the timeout handler.
CVE-2024-40979	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix kernel crash during resume Cu not properly handled, resulting in kernel crash in case DMA remap is not supported: BUG: Bad page state in proce mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x36e80 page dumped because: nonzero _refcount Call T __free_pages_ok __free_pages dma_direct_free dma_free_attrs ath12k_qmi_free_target_mem_chunk ath12k_qmi_ Once ath12k module is loaded, firmware sends memory request to host. In case DMA remap not supported, ath12k in allocating with large segment size: ath12k_pci 0000:04:00.0: qmi firmware request memory request ath12k_pci 7077888 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 8454144 ath12k_pci 0000:04:00.0: qmi dma allocatio with small size ath12k_pci 0000:04:00.0: qmi delays mem_request 2 ath12k_pci 0000:04:00.0: qmi firmware reque back with more but small segments and allocation succeeds: ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 52 seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi m 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_ 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 262144 ath12k_pci 0000:04:00.0: qmi mem seg type 1 mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_ 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_ 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 65536 ath12k_ 524288 Now ath12k is working. If suspend is triggered, firmware will be reloaded during resume. As same as befo first. In ath12k_qmi_msg_mem_request_cb() segment count and size are assigned: ab->qmi.mem_seg_count == 2 >qmi.target_mem[1].size == 8454144 Then allocation failed like before and ath12k_qmi_free_target_mem_chunk(the first segment is skipped because its v.addr is cleared due to allocation failure: chunk->v.addr = dma_alloc_cohe because it has not been freed. While freeing the second segment, a size of 8454144 is passed to dma_free_coherent allocated at the first time firmware is loaded, before suspend. So its real size is 524288, much smaller than 845414 some memory which is in use and thus cras ---truncated---
CVE-2024-40982	In the Linux kernel, the following vulnerability has been resolved: ssb: Fix potential NULL pointer dereference in s function first attempts to convert the 'dev' pointer to 'struct ssb_device *'. However, it mistakenly dereferences 'dev potentially leading to a NULL pointer dereference if 'dev' is NULL. To fix this issue, move the NULL check before the pointer is valid before attempting to use it. Found by Linux Verification Center (linuxtesting.org) with SVACE
CVE-2024-41001	In the Linux kernel, the following vulnerability has been resolved: io_uring/sqpoll: work around a potential audit m there's a memory leak related to connect handling: unreferenced object 0xffff0001093bdf00 (size 128): comm "iou- hex dump (first 32 bytes): 02 00 fa ea 7f 00 00 01 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 0 (crc 2e481b1a): [<00000000c0a26af4>] kmemleak_alloc+0x30/0x38 [<000000009c30bb45>] kmalloc_trace+0x22 __audit_sockaddr+0xd0/0x138 [<0000000089a93e34>] move_addr_to_kernel+0x1a0/0x1f8 [<000000000b4e80e6 [<00000000abfbcd99>] io_submit_sqes+0x588/0x1e48 [<00000000e7c25e07>] io_sq_thread+0x8a4/0x10e4 [<00 +0x10/0x20 which can can happen if: 1) The command type does something on the prep side that triggers an audit before this that triggered an audit call inside ->issue(), where we have audit_uring_entry() and audit_uring_exit(). W operation before the SQPOLL does anything.
CVE-2024-41002	In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/sec - Fix memory leak for sec r resources. When releasing resources, it need to release the AIV resources at the same time. Otherwise, memory lea to the sec resource release function.

CVE-2024-41011	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: don't allow mapping the MMIO H right offset in that case. The GPU has an unused 4K area of the register BAR space into which you can remap regis this space to allow userspace (CPU or GPU) to flush the HDP when it updates VRAM. However, on systems with of MMIO space.
CVE-2024-41013	In the Linux kernel, the following vulnerability has been resolved: xfs: don't walk off the end of a directory data bl xfs_dir2_data_unused and xfs_dir2_data_entry to make sure don't stray beyond valid memory region. Before patch offset of the dup and dep is within the range. So in a crafted image, if last entry is xfs_dir2_data_unused, we can ch 1 byte of space. In the next traversal, this space will be considered as dup or dep. We may encounter an out of boun In the patch, we make sure that the remaining bytes large enough to hold an unused entry before accessing xfs_dir2 XFS_DIR2_DATA_ALIGN byte aligned. We also make sure that the remaining bytes large enough to hold a diren xfs_dir2_data_entry.
CVE-2024-41014	In the Linux kernel, the following vulnerability has been resolved: xfs: add bounds checking to xlog_recover_proce of the space occupied by fixed members of xlog_op_header in the xlog_recover_process_data. We can create a cra bounds read by following these steps: 1) Mount an image of xfs, and do some file operations to leave records 2) Be subsequent steps to simulate abnormal exit. Because umount will ensure that tail_blk and head_blk are the same, w xlog_recover_process_data 3) Write a tool to parse and modify the copied image in step 2 4) Make the end of the x xlog_rec_header->h_size 5) xlog_rec_header->h_num_logops++ 6) Modify xlog_rec_header->h_crc Fix: Add a ch access fixed members of xlog_op_header.
CVE-2024-41015	In the Linux kernel, the following vulnerability has been resolved: ocfs2: add bounds checking to ocfs2_check_dir_ ocfs2_dir_entry to make sure all members of ocfs2_dir_entry don't stray beyond valid memory region.
CVE-2024-41016	In the Linux kernel, the following vulnerability has been resolved: ocfs2: strict bound check before memcmp in ocf 'non-indexed', which saved with additional space requested. It's better to check if the memory is out of bound befor comes from crafted poisonous images.
CVE-2024-41017	In the Linux kernel, the following vulnerability has been resolved: jfs: don't walk off the end of ealist Add a check sure each ea stays within the ealist.
CVE-2024-41019	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Validate ff offset This adds sanity chec >first_free at first, but walking through by ff without any check. If the second ff is a large offset. We may encounte
CVE-2024-41020	In the Linux kernel, the following vulnerability has been resolved: filelock: Fix fcntl/close race recovery compat pa ("filelock: Remove locks reliably when fcntl/close race is detected"), I missed that there are two copies of the code the version for 64-bit offsets on 32-bit kernels. Thanks to Greg KH for stumbling over this while doing the stable b compat path for 32-bit kernels.
CVE-2024-41022	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix signedness bug in sdma_v4_0 needs to be signed for the error handling to work.
CVE-2024-41023	In the Linux kernel, the following vulnerability has been resolved: sched/deadline: Fix task_struct reference leak D test with linux-rt: stress-ng --cyclic 30 --timeout 30 --minimize --quiet kmemleak frequently reported a memory lea object 0xffff8881305b8000 (size 16136): comm "stress-ng", pid 614, jiffies 4294883961 (age 286.412s) object hex 00 00 00 00 00 00 00 00 00 00 .@..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... debug hex 00 00 00 00 00 00 00 00 00 00 S..... backtrace: [<00000000046b6790>] dup_task_struct+0x30/0x540 [<000000 [<00000000ced59777>] kernel_clone+0xb0/0x770 [<00000000a50befdc>] __do_sys_clone+0xb6/0xf0 [<000000 [<00000000552900ff>] entry_SYSCALL_64_after_hwframe+0x6e/0x76 The issue occurs in start_dl_timer(), whi and sets a timer. The timer callback, dl_task_timer, is supposed to decrement the reference count upon expiration. I before the timer expires and cancels it, the reference count is not decremented, leading to the leak. This patch fixes reference count is properly decremented when the timer is canceled.
CVE-2024-41027	In the Linux kernel, the following vulnerability has been resolved: Fix userfaultfd_api to return EINVAL as expect not set in the Kernel config we fail silently and return all the available features. However, the man page indicates w fix this issue since we can end up with a Kernel warning should a program request the feature UFFD_FEATURE_ config not set with this feature. [200.812896] WARNING: CPU: 91 PID: 13634 at mm/memory.c:1660 zap_pte_r linked in: [200.869387] CPU: 91 PID: 13634 Comm: userfaultfd Kdump: loaded Not tainted 6.9.0-rc5+ #8 [200.8 R6525/0N7YGH, BIOS 2.7.3 03/30/2022 [200.885052] RIP: 0010:zap_pte_range+0x43d/0x660
CVE-2024-41030	In the Linux kernel, the following vulnerability has been resolved: ksmbd: discard write access to the directory ope to be opened with the write access. However, some writing flags set by client result in adding write access on serve FUSE file system. Simply, let's discard the write access when opening a directory. list_add corruption. next is NUL BUG at lib/list_debug.c:26! pc : __list_add_valid+0x88/0xbc lr : __list_add_valid+0x88/0xbc Call trace: __list_ad +0x11c/0x170 fuse_open_common+0x284/0x5e8 fuse_dir_open+0x14/0x24 do_dentry_open+0x2a4/0x4e0 dentry handle_ksmbd_work+0x478/0x5ec process_one_work+0x1b4/0x448 worker_thread+0x25c/0x430 kthread+0x104
CVE-2024-41034	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix kernel bug on rename operation of br directory operation on broken directory on nilfs2, __block_write_begin_int() called to prepare block write may fail the folio/page size. This is because nilfs_dotdot(), which gets parent directory reference entry ("..") of the directory consistency enough, and may return location exceeding folio/page size for broken directories. Fix this issue by che in the first chunk of the directory in nilfs_dotdot().

CVE-2024-41035	In the Linux kernel, the following vulnerability has been resolved: USB: core: Fix duplicate endpoint bug by cleari identified a bug in usbcore (see the Closes: tag below) caused by our assumption that the reserved bits in an endpoi always be 0. As a result of the bug, the endpoint_is_duplicate() routine in config.c (and possibly other routines as v for distinct endpoints, even though they have the same direction and endpoint number. This can lead to confusion, descriptors with matching endpoint numbers and directions, where one was interrupt and the other was bulk). To fi bEndpointAddress when we parse the descriptor. (Note that both the USB-2.0 and USB-3.1 specs say these bits are to make a copy of the descriptor earlier in usb_parse_endpoint() and use the copy instead of the original when chec
CVE-2024-41036	In the Linux kernel, the following vulnerability has been resolved: net: ks8851: Fix deadlock with the SPI chip vari are actually functional then there is a deadlock with the 'statelock' spinlock between ks8851_start_xmit_spi and ks8 lockup - CPU#0 stuck for 27s! call trace: queued_spin_lock_slowpath+0x100/0x284 do_raw_spin_lock+0x34/0x4 ks8851_start_xmit+0x14/0x20 netdev_start_xmit+0x40/0x6c dev_hard_start_xmit+0x6c/0xbc sch_direct_xmit+0x qdisc_run+0x24/0x3c net_tx_action+0xf8/0x130 handle_softirqs+0x1ac/0x1f0 __do_softirq+0x14/0x20 ____do_s +0x3c/0x58 do_softirq_own_stack+0x1c/0x28 __irq_exit_rcu+0x54/0x9c irq_exit_rcu+0x10/0x1c el1_interrupt+0 el1h_64_irq+0x64/0x68 __netif_schedule+0x6c/0x80 netif_tx_wake_queue+0x38/0x48 ks8851_irq+0xb8/0x2c8 i +0x10c/0x1b0 kthread+0xc8/0xd8 ret_from_fork+0x10/0x20 This issue has not been identified earlier because test and so spinlocks were actually NOPs. Now use spin_(un)lock_bh for TX queue related locking to avoid execution to a deadlock.
CVE-2024-41040	In the Linux kernel, the following vulnerability has been resolved: net/sched: Fix UAF when resolving a clash KAS BUG: KASAN: slab-use-after-free in tcf_ct_flow_table_process_conn+0x12b/0x380 [act_ct] Read of size 1 at add handler130/6469 Call Trace: <IRQ> dump_stack_lvl+0x48/0x70 print_address_description.constprop.0+0x33/0x3 +0xd0/0x120 __asan_load1+0x6c/0x80 tcf_ct_flow_table_process_conn+0x12b/0x380 [act_ct] tcf_ct_act+0x886/(+0xf8/0x1f0 fl_classify+0x355/0x360 [cls_flower] __tcf_classify+0x1fd/0x330 tcf_classify+0x21c/0x3c0 sch_han __netif_receive_skb_core.constprop.0+0xb25/0x1510 __netif_receive_skb_list_core+0x220/0x4c0 netif_receive_s napi_complete_done+0x157/0x3d0 gro_cell_poll+0xcf/0x100 __napi_poll+0x65/0x310 net_rx_action+0x30c/0x5c +0x82/0xc0 irq_exit_rcu+0xe/0x20 common_interrupt+0xa1/0xb0 </IRQ> <TASK> asm_common_interrupt+0x2 kasan_save_stack+0x38/0x70 kasan_set_track+0x25/0x40 kasan_save_alloc_info+0x1e/0x40 __kasan_krealloc+0 nf_ct_ext_add+0xed/0x230 [nf_conntrack] tcf_ct_act+0x1095/0x1350 [act_ct] tcf_action_exec+0xf8/0x1f0 fl_clas __tcf_classify+0x1fd/0x330 tcf_classify+0x21c/0x3c0 sch_handle_ingress.constprop.0+0x2c5/0x500 __netif_rece __netif_receive_skb_list_core+0x220/0x4c0 netif_receive_skb_list_internal+0x446/0x620 napi_complete_done+0 __napi_poll+0x65/0x310 net_rx_action+0x30c/0x5c0 __do_softirq+0x14f/0x491 Freed by task 6469: kasan_save_ +0x25/0x40 kasan_save_free_info+0x2b/0x60 ____kasan_slab_free+0x180/0x1f0 __kasan_slab_free+0x12/0x30 s __kmem_cache_free+0x1a2/0x2f0 kfree+0x78/0x120 nf_conntrack_free+0x74/0x130 [nf_conntrack] nf_ct_destro __nf_ct_resolve_clash+0x529/0x5d0 [nf_conntrack] nf_ct_resolve_clash+0xf6/0x490 [nf_conntrack] __nf_conntra tcf_ct_act+0x12ad/0x1350 [act_ct] tcf_action_exec+0xf8/0x1f0 fl_classify+0x355/0x360 [cls_flower] __tcf_classi sch_handle_ingress.constprop.0+0x2c5/0x500 __netif_receive_skb_core.constprop.0+0xb25/0x1510 __netif_recei netif_receive_skb_list_internal+0x446/0x620 napi_complete_done+0x157/0x3d0 gro_cell_poll+0xcf/0x100 __nap +0x30c/0x5c0 __do_softirq+0x14f/0x491 The ct may be dropped if a clash has been resolved but is still passed to t for further usage. This issue can be fixed by retrieving ct from skb again after confirming conntrack.
CVE-2024-41041	In the Linux kernel, the following vulnerability has been resolved: udp: Set SOCK_RCU_FREE earlier in udp_lib_ [0] in udp_v4_early_demux(). In udp_v[46]_early_demux() and sk_lookup(), we do not touch the refcount of the lo skb->destructor, so we check SOCK_RCU_FREE to ensure that the sk is safe to access during the RCU grace perio flagged for a bound socket after being put into the hash table. Moreover, the SOCK_RCU_FREE check is done too and sk_lookup(), so there could be a small race window: CPU1 CPU2 ---- ---- udp_v4_early_demux() udp_lib_get_ __udp4_lib_demux_lookup() | |- DEBUG_NET_WARN_ON_ONCE(sk_is_refcounted(sk)); `- sock_set_flag(sk, S bug in TCP and fixed it in commit 871019b22d1b ("net: set SOCK_RCU_FREE before inserting socket into hashta [0]: WARNING: CPU: 0 PID: 11198 at net/ipv4/udp.c:2599 udp_v4_early_demux+0x481/0xb70 net/ipv4/udp.c:25 11198 Comm: syz-executor.1 Not tainted 6.9.0-g93bda33046e7 #13 Hardware name: QEMU Standard PC (i440FX gd239552ce722-prebuilt.qemu.org 04/01/2014 RIP: 0010:udp_v4_early_demux+0x481/0xb70 net/ipv4/udp.c:2599 e9 31 ff d3 e3 81 e3 bf ef ff ff 89 de e8 2c 74 15 fe 85 db 0f 85 02 06 00 00 e8 9f 7a 15 fe <0f> 0b e8 98 7a 15 fe 4 52 RSP: 0018:ffffc9000ce3fa58 EFLAGS: 00010293 RAX: 0000000000000000 RBX: 0000000000000000 RCX: RSI: ffffffff8318c2f1 RDI: 0000000000000001 RBP: ffff88805a2dd6e0 R08: 0000000000000001 R09: 0000000(R11: 0001ffffffffffff R12: ffff88805a2dd680 R13: 0000000000000007 R14: ffff88800923f900 R15: ffff888054560 GS:ffff88807dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 C 000000003de4b002 CR4: 0000000000770ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000(00000000fffe0ff0 DR7: 0000000000000600 PKRU: 55555554 Call Trace: <TASK> ip_rcv_finish_core.constprop ip_rcv_finish+0xda/0x150 net/ipv4/ip_input.c:447 NF_HOOK include/linux/netfilter.h:314 [inline] NF_HOOK inc +0x16c/0x180 net/ipv4/ip_input.c:569 __netif_receive_skb_one_core+0xb3/0xe0 net/core/dev.c:5624 __netif_rece netif_receive_skb_internal net/core/dev.c:5824 [inline] netif_receive_skb+0x271/0x300 net/core/dev.c:5884 tun_rx tun_get_user+0x24db/0x2c50 drivers/net/tun.c:2002 tun_chr_write_iter+0x107/0x1a0 drivers/net/tun.c:2048 new_ vfs_write+0x76f/0x8d0 fs/read_write.c:590 ksys_write+0xbf/0x190 fs/read_write.c:643 __do_sys_write fs/read_w read_write.c:652 [inline] __x64_sys_write+0x41/0x50 fs/read_write.c:652 x64_sys_call+0xe66/0x1990 arch/x86/i do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x4b/0x110 arch/x86/entry/common.c:83 entr RIP: 0033:0x7fc44a68bc1f Code: 89 54 24 18 48 89 74 24 10 89 7c 24 08 e8 e9 cf f5 ff 48 8b 54 24 18 48 8b 74 24 05 <48> 3d 00 f0 ff ff 77 31 44 89 c7 48 89 44 24 08 e8 3c d0 f5 ff 48 RSP: 002b:00007fc449126c90 EFLAGS: 00 RAX: ffffffffffffffda RBX: 00000000004bc050 RCX: 00007fc44a68bc1f R ---truncated---

CVE-2024-41042	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: prefer nft_chain_validate nf detection because a cycle will result in a call stack overflow (ctx->level >= NFT_JUMP_STACK_SIZE). It also fo nft_lookup, so there appears no reason to iterate the maps again. nf_tables_check_loops() and all its helper functio time significantly, from 23s down to 12s. This also fixes a crash bug. Old loop detection code can result in unboun was hit at .... Oops: stack guard page: 0000 [#1] PREEMPT SMP KASAN CPU: 4 PID: 1539 Comm: nft Not tainte during validation of register stores. I can't see any actual reason to attempt to check for this from nft_validate_regis in progress, so we don't have a full picture of the rule graph. For nf-next it might make sense to either remove it or case we could catch an error earlier (for improved error reporting to userspace).
CVE-2024-41044	In the Linux kernel, the following vulnerability has been resolved: ppp: reject claimed-as-LCP but actually malform assumes valid LCP packets (with code from 1 to 7 inclusive), add 'ppp_check_packet()' to ensure that LCP packet h bytes, and reject claimed-as-LCP but actually malformed data otherwise.
CVE-2024-41046	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: lantiq_etop: fix double free in deta descriptor is never incremented which results in the same skb being released multiple times.
CVE-2024-41048	In the Linux kernel, the following vulnerability has been resolved: skmsg: Skip zero length skb in sk_msg_recvmsg t sockmap_basic) on a Loongarch platform, the following kernel panic occurs: [...] Oops[#1]: CPU: 22 PID: 2824 C #18 Hardware name: LOONGSON Dabieshan/Loongson-TC542F0, BIOS Loongson-UDK2018 ... ... ra: 90000000 ERA: 9000000004162774 copy_page_to_iter+0x74/0x1c0 CRMD: 000000b0 (PLV0 -IE -DA +PG DACF=CC DA (PPLV0 +PIE +PWE) EUEN: 00000007 (+FPE +SXE +ASXE -BTE) ECFG: 00071c1d (LIE=0,2-4,10-12 VS=7) EsubCode=0) BADV: 0000000000000040 PRID: 0014c011 (Loongson-64bit, Loongson-3C5000) Modules linked xt_MASQUERADE xt_conntrack Process test_progs (pid: 2824, threadinfo=0000000000863a31, task=...) Stack : copy_page_to_iter+0x74/0x1c0 [<90000000048bf6c0>] sk_msg_recvmsg+0x120/0x560 [<90000000049f2b90>] t [<90000000049aae34>] inet_recvmsg+0x54/0x100 [<900000000481ad5c>] sock_recvmsg+0x7c/0xe0 [<9000000 [<900000000481e27c>] sys_recvfrom+0x1c/0x40 [<9000000004c076ec>] do_syscall+0x8c/0xc0 [<900000003 ---[end trace 0000000000000000]--- Kernel panic - not syncing: Fatal exception Kernel relocated by 0x3510000 . 0x9000000004d70000 .bss @ 0x9000000006469400 ---[end Kernel panic - not syncing: Fatal exception]--- [...] T sockmap_skb_verdict_shutdown subtest in sockmap_basic. This crash is because a NULL pointer is passed to page to the different implementations depending on the architecture, page_address(NULL) will trigger a panic on Loong this bug was hidden on x86 platform for a while, but now it is exposed on Loongarch platform. The root cause is th put on the queue. This zero length skb is a TCP FIN packet, which was sent by shutdown(), invoked in test_sockma SHUT_WR); In this case, in sk_psock_skb_ingress_enqueue(), num_sge is zero, and no page is put to this sge (see empty sge is queued into ingress_msg list. And in sk_msg_recvmsg(), this empty sge is used, and a NULL page is to copy_page_to_iter(), which passes it to kmap_local_page() and to page_address(), then kernel panics. To solve t So in sk_msg_recvmsg(), if copy is zero, that means it's a zero length skb, skip invoking copy_page_to_iter(). We a copy_page_to_iter to check for is_fin in tcp_bpf.c.
CVE-2024-41049	In the Linux kernel, the following vulnerability has been resolved: filelock: fix potential use-after-free in posix_loc warning in trace_posix_lock_inode(). The request pointer had been changed earlier to point to a lock entry that was the tracepoint could fire, another task raced in and freed that lock. Fix this by moving the tracepoint inside the spin happen.
CVE-2024-41055	In the Linux kernel, the following vulnerability has been resolved: mm: prevent derefencing NULL ptr in pfn_secti sparsemem: fix race in accessing memory_section->usage") changed pfn_section_valid() to add a READ_ONCE() section_deactivate() where ms->usage can be cleared. The READ_ONCE() call, by itself, is not enough to prevent its value before dereferencing it.
CVE-2024-41059	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix uninit-value in copy_name [syzbot r value in sized_strscpy+0xc4/0x160 sized_strscpy+0xc4/0x160 copy_name+0x2af/0x320 fs/hfsplus/xattr.c:411 hfsp hfsplus/xattr.c:750 vfs_listxattr fs/xattr.c:493 [inline] listxattr+0x1f3/0x6b0 fs/xattr.c:840 path_listxattr fs/xattr.c:8 xattr.c:876 [inline] __se_sys_listxattr fs/xattr.c:873 [inline] __x64_sys_listxattr+0x16b/0x2f0 fs/xattr.c:873 x64_sy include/generated/asm/syscalls_64.h:195 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xc entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3877 [inl kmalloc_trace+0x57b/0xbe0 mm/slub.c:4065 kmalloc include/linux/slab.h:628 [inline] hfsplus_listxattr+0x4cc/0x1 fs/xattr.c:493 [inline] listxattr+0x1f3/0x6b0 fs/xattr.c:840 path_listxattr fs/xattr.c:864 [inline] __do_sys_listxattr fs/ fs/xattr.c:873 [inline] __x64_sys_listxattr+0x16b/0x2f0 fs/xattr.c:873 x64_sys_call+0x2ba0/0x3b50 arch/x86/inclu do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entr [Fix] When allocating memory to strbuf, initialize memory to 0.
CVE-2024-41060	In the Linux kernel, the following vulnerability has been resolved: drm/radeon: check bo_va->bo is non-NULL bef radeon_vm_clear_freed might clear bo_va->bo, so we have to check it before dereferencing it.
CVE-2024-41061	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix array-index-out-of-bounds Potential out of bounds access in dml2_calculate_rq_and_dlg_params() because the value of out_lowest_state_idx array can be greater than 1. [How] Currently dml2 core specifies identical values for all FCLKChangeSupport elem avoid out of bounds access.

CVE-2024-41062	In the Linux kernel, the following vulnerability has been resolved: bluetooth/l2cap: sync sock recv cb and release T call to close the sock and hci_rx_work, where the former releases the sock and the latter accesses it without lock pr hci_rx_work l2cap_sock_release hci_acldata_packet l2cap_sock_kill l2cap_recv_frame sk_free l2cap_conless_cha processes the data that needs to be received before the sock is closed, then everything is normal; Otherwise, the wo receiving data. Add a chan mutex in the rx callback of the sock to achieve synchronization between the sock releas to NULL, avoid others use invalid sock pointer.
CVE-2024-41063	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: cancel all works upon hci_ calling hci_release_dev() from hci_error_reset() due to hci_dev_put() from hci_error_reset() can cause deadlock at is called from hdev->req_workqueue which destroy_workqueue() needs to flush. We need to make sure that hdev-> are queued into hdev->workqueue and hdev->{power_on,error_reset} which are queued into hdev->req_workqueu destroy_workqueue(hdev->workqueue); destroy_workqueue(hdev->req_workqueue); are called from hci_release_ items from hci_unregister_dev() as soon as hdev->list is removed from hci_dev_list.
CVE-2024-41064	In the Linux kernel, the following vulnerability has been resolved: powerpc/eeh: avoid possible crash when edev-> during eeh_pe_report_edev(), edev->pdev will change and can cause a crash, hold the PCI rescan/remove lock whi
CVE-2024-41065	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Whitelist dtl slub object for co trace log from /sys/kernel/debug/powerpc/dtl/cpu-* results in a BUG() when the config CONFIG_HARDENED_U kernel BUG at mm/usercopy.c:102! Oops: Exception in kernel mode, sig: 5 [#1] LE PAGE_SIZE=64K MMU=Rad Modules linked in: xfs libcrc32c dm_service_time sd_mod t10_pi sg ibmvfc scsi_transport_fc ibmveth pseries_wd dm_log dm_mod fuse CPU: 27 PID: 1815 Comm: python3 Not tainted 6.10.0-rc3 #85 Hardware name: IBM,9040- of:IBM,FW1060.00 (NM1060_042) hv:phyp pSeries NIP: c0000000005d23d4 LR: c0000000005d23d0 CTR: 0000 TRAP: 0700 Not tainted (6.10.0-rc3) MSR: 8000000000029033 <SF,EE,ME,IR,DR,RI,LE> CR: 2828220f XER: 0 IRQMASK: 0 [... GPRs omitted ...] NIP [c0000000005d23d4] usercopy_abort+0x78/0xb0 LR [c0000000005d23d usercopy_abort+0x74/0xb0 (unreliable) __check_heap_object+0xf8/0x120 check_heap_object+0x218/0x240 __ch +0x17c/0x2c4 full_proxy_read+0x8c/0x110 vfs_read+0xdc/0x3a0 ksys_read+0x84/0x144 system_call_exception+ +0x15c/0x2ec --- interrupt: 3000 at 0x7fff81f3ab34 Commit 6d07d1cd300f ("usercopy: Restrict non-usercopy cach whitelisted areas in slab/slub objects can be copied to userspace when usercopy hardening is enabled using CONFI contains hypervisor dispatch events which are expected to be read by privileged users. Hence mark this safe for use usersize=DISPATCH_LOG_BYTES to whitelist the entire object.
CVE-2024-41066	In the Linux kernel, the following vulnerability has been resolved: ibmvnic: Add tx check to prevent skb leak Belo a reference to an skb during transmit: tx_buff[free_map[consumer_index]]->skb = new_skb; free_map[consumer_i consumer_index ++; Where variable data looks like this: free_map == [4, IBMVNIC_INVALID_MAP, IBMVNIC tx_buff == [skb=null, skb=<ptr>, skb=<ptr>, skb=null, skb=null] The driver has checks to ensure that free_map[co there was no check to ensure that this index pointed to an unused/null skb address. So, if, by some chance, our free then we were previously risking an skb memory leak. This could then cause tcp congestion control to stop sending Therefore, add a conditional to ensure that the skb address is null. If not then warn the user (because this is still a b pointer to prevent memleak/tcp problems.
CVE-2024-41067	In the Linux kernel, the following vulnerability has been resolved: btrfs: scrub: handle RST lookup error correctly RST feature, it would crash the following ASSERT() inside scrub_read_endio(): ASSERT(sector_nr < stripe->nr_s dump from btrfs_get_raid_extent_offset(), as we failed to find the RST entry for the range. [CAUSE] Inside scrub_ allocated a new bbio we immediately called btrfs_map_block() to make sure there was some RST range covering th we immediately call endio for the bbio, while the bbio is newly allocated, it's completely empty. Then inside scrub_ find the sector number (as bi_sector is no longer reliable if the bio is submitted to lower layers). And since the bio i any sector matching the sector, and return sector_nr == stripe->nr_sectors, triggering the ASSERT(). [FIX] Instead a new bbio, call btrfs_map_block() first. Since our only objective of calling btrfs_map_block() is only to update str btrfs_alloc_bio(). This new timing would avoid the problem of handling empty bbio completely, and in fact fixes a if the submission thread is the only owner of the pending_io, the scrub would never finish (since we didn't decrease cause of RST lookup failure still needs to be addressed.
CVE-2024-41068	In the Linux kernel, the following vulnerability has been resolved: s390/sclp: Fix sclp_init() cleanup on failure If sc up: if there are multiple failing calls to sclp_init() sclp_state_change_event will be added several times to sclp_reg_ warning: ------------[cut here]------------ list_add double add: new=000003ffe1598c10, prev=000003ffe1598bf0, ne CPU: 0 PID: 1 at lib/list_debug.c:35 __list_add_valid_or_report+0xde/0xf8 CPU: 0 PID: 1 Comm: swapper/0 Not 0404c00180000000 000003ffe0d6076a (__list_add_valid_or_report+0xe2/0xf8) R:0 T:1 IO:0 EX:0 Key:0 M:1 W: Trace: [<000003ffe0d6076a>] __list_add_valid_or_report+0xe2/0xf8 ([<000003ffe0d60766>] __list_add_valid_or sclp_init+0x40e/0x450 [<000003ffe00009f2>] do_one_initcall+0x42/0x1e0 [<000003ffe15b77a6>] do_initcalls+0 kernel_init_freeable+0x1ba/0x1f8 [<000003ffe0d6650e>] kernel_init+0x2e/0x180 [<000003ffe000301c>] __ret_fr ret_from_fork+0xa/0x30 Fix this by removing sclp_state_change_event from sclp_reg_list when sclp_init() fails.
CVE-2024-41069	In the Linux kernel, the following vulnerability has been resolved: ASoC: topology: Fix references to freed memor release memory used by it, so having pointer references directly into topology file contents is wrong. Use devm_km

CVE-2024-41070	In the Linux kernel, the following vulnerability has been resolved: KVM: PPC: Book3S HV: Prevent UAF in kvm_ Al reported a possible use-after-free (UAF) in kvm_spapr_tce_attach_iommu_group(). It looks up `stt` from tablefd doing fdput() on the returned fd. After the fdput() the tablefd is free to be closed by another thread. The close calls release_spapr_tce_table() (via call_rcu()) which frees `stt`. Although there are calls to rcu_read_lock() in kvm_spa not sufficient to prevent the UAF, because `stt` is used outside the locked regions. With an artifcial delay after the triggers the race, KASAN detects the UAF: BUG: KASAN: slab-use-after-free in kvm_spapr_tce_attach_iommu_ addr c000200027552c30 by task kvm-vfio/2505 CPU: 54 PID: 2505 Comm: kvm-vfio Not tainted 6.10.0-rc3-next- GTH POWER9 0x4e1202 opal:skiboot-v6.5.3-35-g1851b2a06 PowerNV Call Trace: dump_stack_lvl+0xb4/0x108 kasan_report+0x118/0x2b0 __asan_load4+0xb8/0xd0 kvm_spapr_tce_attach_iommu_group+0x298/0x720 [kvm] kvm_device_ioctl+0x144/0x240 [kvm] sys_ioctl+0x62c/0x1810 system_call_exception+0x190/0x440 system_call by task 0: ... kfree+0xec/0x3e0 release_spapr_tce_table+0xd4/0x11c [kvm] rcu_core+0x568/0x16a0 handle_softirq +0x6c/0x90 do_softirq_own_stack+0x58/0x90 __irq_exit_rcu+0x218/0x2d0 irq_exit+0x30/0x80 arch_local_irq_re +0x1c/0x30 cpuidle_enter_state+0x134/0x5cc cpuidle_enter+0x6c/0xb0 call_cpuidle+0x7c/0x100 do_idle+0x394/ start_secondary+0x3fc/0x410 start_secondary_prolog+0x10/0x14 Fix it by delaying the fdput() until `stt` is no long function. To keep the patch minimal add a call to fdput() at each of the existing return paths. Future work can conv cleanup. With the fix in place the test case no longer triggers the UAF.
CVE-2024-41071	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: Avoid address calculations via >n_channels must be set before req->channels[] can be used. This patch fixes one of the issues encountered in [1]. bounds in net/mac80211/scan.c:364:4 [83.964258] index 0 is out of range for type 'struct ieee80211_channel *[]' [<TASK> [83.964269] dump_stack_lvl+0x3f/0xc0 [83.964274] __ubsan_handle_out_of_bounds+0xec/0x110 [83 +0x2db/0x4b0 [83.964281] __ieee80211_start_scan+0x601/0x990 [83.964291] nl80211_trigger_scan+0x874/0x9 +0xe8/0x160 [83.964298] genl_rcv_msg+0x240/0x270 [...] [1] https://bugzilla.kernel.org/show_bug.cgi?id=21881
CVE-2024-41072	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: wext: add extra SIOCSIWSCAN add extra check whether number of channels passed via 'ioctl(sock, SIOCSIWSCAN, ...)' doesn't exceed IW_MAX with -EINVAL otherwise.
CVE-2024-41073	In the Linux kernel, the following vulnerability has been resolved: nvme: avoid double free special payload If a dis may fail before a new special payload is added, a double free will result. Clear the RQF_SPECIAL_LOAD when th
CVE-2024-41074	In the Linux kernel, the following vulnerability has been resolved: cachefiles: Set object to close if ondemand_id < the user mode, it may delete the request corresponding to the random id. And the request may have not been read y the open request will be done with the still reopen state in above case. As a result, the request corresponding to this function, so the read request is never completed and blocks other process. Fix this issue by simply set object to clos
CVE-2024-41075	In the Linux kernel, the following vulnerability has been resolved: cachefiles: add consistency check for copen/crea completing random copen/cread requests and crashing the system. Added checks are listed below: * Generic, copen can only complete read requests. * For copen, ondemand_id must not be 0, because this indicates that the request h the object corresponding to fd and req should be the same.
CVE-2024-41076	In the Linux kernel, the following vulnerability has been resolved: NFSv4: Fix memory leak in nfs4_set_security_l time we set a security xattr.
CVE-2024-41077	In the Linux kernel, the following vulnerability has been resolved: null_blk: fix validation of block size Block size be a power of 2. The current check does not validate this, so update the check. Without this patch, null_blk would with bs=1536 [1]. [axboe: remove unnecessary braces and != 0 check]
CVE-2024-41078	In the Linux kernel, the following vulnerability has been resolved: btrfs: qgroup: fix quota root leak after quota disa fail when cleaning the quota tree or when deleting the root from the root tree, we jump to the 'out' label without eve resulting in a leak of the root since fs_info->quota_root is no longer pointing to the root (we have set it to NULL ju doing a btrfs_put_root() call under the 'out' label. This is a problem that exists since qgroups were first added in 20 implementation and prototypes"), but back then we missed a kfree on the quota root and free_extent_buffer() calls then roots were not yet reference counted.
CVE-2024-41079	In the Linux kernel, the following vulnerability has been resolved: nvmet: always initialize cqe.result The spec doe (aka results) for the command queue entry need to be set to 0 when they are not used (not specified). Though, the ta but not for RDMA. Let's make RDMA behave the same and thus explicitly initializing the result field. This preven
CVE-2024-41080	In the Linux kernel, the following vulnerability has been resolved: io_uring: fix possible deadlock in io_register_io io_register_iowq_max_workers() function calls io_put_sq_data(), which acquires the sqd->lock without releasing t 009ad9f0c6ee ("io_uring: drop ctx->uring_lock before acquiring sqd->lock"), this can lead to a potential deadlock is released before calling io_put_sq_data(), and then it is re-acquired after the function call. This change ensures tha preventing the possibility of a deadlock.
CVE-2024-41081	In the Linux kernel, the following vulnerability has been resolved: ila: block BH in ila_output() As explained in co before using dst_cache"), net/core/dst_cache.c helpers need to be called with BH disabled. ila_output() is called fro context, and under rcu_read_lock(). We might be interrupted by a softirq, re-enter ila_output() and corrupt dst_cach local_bh_disable().

CVE-2024-41082	In the Linux kernel, the following vulnerability has been resolved: nvme-fabrics: use reserved tag for reg read/writ commands are issued by nvme command in the same time by user tasks, this may exhaust all tags of admin_q. If a before these commands finish, reconnect routine may fail to update nvme regs due to insufficient tags, which will workaround this issue, maybe we can let reg_read32()/reg_read64()/reg_write32() use reserved tags. This maybe sa will not issue connect command 2. For the enable ctrl / fw activate path, since connect and reg_xx() are called seria while reg_xx() use reserved tags.
CVE-2024-41087	In the Linux kernel, the following vulnerability has been resolved: ata: libata-core: Fix double free on error If e.g. t fails, we will jump to the err_out label, which will call devres_release_group(). devres_release_group() will trigger ata_host_release() calls kfree(host), so executing the kfree(host) in ata_host_alloc() will lead to a double free: kern opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 11 PID: 599 Comm: (udev-worker) Not tainted 6.10.0-rc5 #47 H + PIIX, 1996), BIOS 1.16.3-2.fc40 04/01/2014 RIP: 0010:kfree+0x2cf/0x2f0 Code: 5d 41 5e 41 5f 5d e9 80 d6 ff f 89 da RSP: 0018:ffffc90000f377f0 EFLAGS: 00010246 RAX: ffff888112b1f2c0 RBX: ffff888112b1f2c0 RCX: ff RSI: ffffffffc02c9de5 RDI: ffff888112b1f2c0 RBP: ffffc90000f37830 R08: 0000000000000000 R09: 0000000000 617461203a736b6e R12: ffffea00044ac780 R13: ffff888100046400 R14: ffffffffc02c9de5 R15: 000000000000000 GS:ffff88813b380000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 C 0000000111724000 CR4: 0000000000750ef0 PKRU: 55555554 Call Trace: <TASK> ? __die_body.cold+0x19/0x do_error_trap+0x6a/0x90 ? kfree+0x2cf/0x2f0 ? exc_invalid_op+0x50/0x70 ? kfree+0x2cf/0x2f0 ? asm_exc_inval +0xf5/0x120 [libata] ? ata_host_alloc+0xf5/0x120 [libata] ? kfree+0x2cf/0x2f0 ata_host_alloc+0xf5/0x120 [libata] ahci_init_one+0x6c9/0xd20 [ahci] Ensure that we will not call kfree(host) twice, by performing the kfree() only if
CVE-2024-41088	In the Linux kernel, the following vulnerability has been resolved: can: mcp251xfd: fix infinite loop when xmit fai function fails, the driver stops processing messages, and the interrupt routine does not return, running indefinitely e Error messages: [441.298819] mcp251xfd spi2.0 can0: ERROR in mcp251xfd_start_xmit: -16 [441.306498] mcp buffer not empty. (seq=0x000017c7, tef_tail=0x000017cf, tef_head=0x000017d0, tx_head=0x000017d3). ... and re when multiple devices share the same SPI interface. And there is concurrent access to the bus. The problem occurs mcp251xfd_start_xmit() fails. Consequently, the driver skips one TX package while still expecting a response in m issue by starting a workqueue to write the tx obj synchronously if err = -EBUSY. In case of another error, decreme stack, and drop the message. [mkl: use more imperative wording in patch description]
CVE-2024-41089	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau/dispnv04: fix null pointer derefere nv17_tv_get_hd_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a poss drm_mode_duplicate(). The same applies to drm_cvt_mode(). Add a check to avoid null pointer dereference.
CVE-2024-41092	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: Fix potential UAF by revoke of fer reporting the following issue triggered by igt@i915_selftest@live@hangcheck on ADL-P and similar machines: <6 intel_hangcheck_live_selftests/igt_reset_evict_fence ... <6> [414.068804] i915 0000:00:02.0: [drm] GT0: GUC: su i915 0000:00:02.0: [drm] GT0: GUC: SLPC enabled <3> [414.070354] Unable to pin Y-tiled fence; err:-4 <3> [41 GEM_BUG_ON(!i915_active_is_idle(&fence->active)) ... <4>[609.603992] ------------[cut here]------------ <2>[gpu/drm/i915/gt/intel_ggtt_fencing.c:301! <4>[609.604003] invalid opcode: 0000 [#1] PREEMPT SMP NOPTI < Comm: kworker/u64:3 Tainted: G U W 6.9.0-CI_DRM_14785-g1ba62f8cea9c+ #1 <4>[609.604008] Hardware na Platform/AlderLake-P DDR4 RVP, BIOS RPLPFWI1.R00.4035.A00.2301200723 01/20/2023 <4>[609.604010] V [i915] <4>[609.604149] RIP: 0010:i915_vma_revoke_fence+0x187/0x1f0 [i915] ... <4>[609.604271] Call Trace: <4>[609.604716] __i915_vma_evict+0x2e9/0x550 [i915] <4>[609.604852] __i915_vma_unbind+0x7c/0x160 [i9 +0x24/0xa0 [i915] <4>[609.605098] i915_vma_destroy+0x2f/0xa0 [i915] <4>[609.605210] __i915_gem_object_ <4>[609.605330] __i915_gem_free_objects.isra.0+0x6a/0xc0 [i915] <4>[609.605440] process_scheduled_works similar failures reported by CI from other IGT tests, observed on other platforms. Before commit 63baf4f3d587 ("d before unbinding a GGTT fence"), i915_vma_revoke_fence() was waiting for idleness of vma->active via fence_up >active in order for the fence_update() to be able to wait selectively on that one instead of vma->active since only i then, another commit 0d86ee35097a ("drm/i915/gt: Make fence revocation unequivocal") replaced the call to fence with only fence_write(), and also added that GEM_BUG_ON(!i915_active_is_idle(&fence->active)) in front. No ju might then expect idleness of vma->fence->active without first waiting on it. The issue can be potentially caused by registers on one side and sequential execution of signal callbacks invoked on completion of a request that was using parallel to revocation of those fence registers. Fix it by waiting for idleness of vma->fence->active in i915_vma_re 24bb052d3dd499c5956abad5f7d8e4fd07da7fb1)
CVE-2024-41093	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: avoid using null object of framebu directly, get object from framebuffer by calling drm_gem_fb_get_obj() and return error code when object is null to
CVE-2024-41095	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau/dispnv04: fix null pointer derefere nv17_tv_get_ld_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possi drm_mode_duplicate(). Add a check to avoid npd.

CVE-2024-41097	In the Linux kernel, the following vulnerability has been resolved: usb: atm: cxacru: fix endpoint checking in cxacr an old issue [1] that occurs due to incomplete checking of present usb endpoints. As such, wrong endpoints types n in turn triggers a warning in usb_submit_urb(). Fix the issue by verifying that required endpoint types are present f account cmd endpoint type. Unfortunately, this patch has not been tested on real hardware. [1] Syzbot report: usb 1 WARNING: CPU: 0 PID: 8667 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb. Comm: kworker/0:4 Not tainted 5.14.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Workqueue: usb_hub_wq hub_event RIP: 0010:usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502 ... Call atm/cxacru.c:649 cxacru_card_status+0x22/0xd0 drivers/usb/atm/cxacru.c:760 cxacru_bind+0x7ac/0x11a0 drivers +0x321/0x1ae0 drivers/usb/atm/usbatm.c:1055 cxacru_usb_probe+0xdf/0x1e0 drivers/usb/atm/cxacru.c:1363 usb_ core/driver.c:396 call_driver_probe drivers/base/dd.c:517 [inline] really_probe+0x23c/0xcd0 drivers/base/dd.c:595 drivers/base/dd.c:747 driver_probe_device+0x4c/0x1a0 drivers/base/dd.c:777 __device_attach_driver+0x20b/0x2f +0x15f/0x1e0 drivers/base/bus.c:427 __device_attach+0x228/0x4a0 drivers/base/dd.c:965 bus_probe_device+0x1e +0xc2f/0x2180 drivers/base/core.c:3354 usb_set_configuration+0x113a/0x1910 drivers/usb/core/message.c:2170 u drivers/usb/core/generic.c:238 usb_probe_device+0xd9/0x2c0 drivers/usb/core/driver.c:293
CVE-2024-41098	In the Linux kernel, the following vulnerability has been resolved: ata: libata-core: Fix null pointer dereference on ata_host_alloc() fails, ata_host_release() will get called. However, the code in ata_host_release() tries to free ata_p can lead to the following: BUG: unable to handle page fault for address: 0000000000003990 PGD 0 P4D 0 Oops: CPU: 10 PID: 594 Comm: (udev-worker) Not tainted 6.10.0-rc5 #44 Hardware name: QEMU Standard PC (i440F 04/01/2014 RIP: 0010:ata_host_release.cold+0x2f/0x6e [libata] Code: e4 4d 63 f4 44 89 e2 48 c7 c6 90 ad 32 c0 4 0018:ffffc90000ebb968 EFLAGS: 00010246 RAX: 0000000000000041 RBX: ffff88810fb52e78 RCX: 000000000 RSI: ffff88813b3218c0 RDI: ffff88813b3218c0 RBP: ffff88810fb52e40 R08: 0000000000000000 R09: 6c65725f7 73692033203a746e R12: 0000000000000004 R13: 0000000000000000 R14: 0000000000000011 R15: 000000000 GS:ffff88813b300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 C 00000001122a2000 CR4: 0000000000750ef0 PKRU: 55555554 Call Trace: <TASK> ? __die_body.cold+0x19/0x exc_page_fault+0x7e/0x180 ? asm_exc_page_fault+0x26/0x30 ? ata_host_release.cold+0x2f/0x6e [libata] ? ata_h release_nodes+0x35/0xb0 devres_release_group+0x113/0x140 ata_host_alloc+0xed/0x120 [libata] ata_host_alloc_ +0x6c9/0xd20 [ahci] Do not access ata_port struct members unconditionally.
CVE-2024-42063	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark bpf prog stack with kmsan_unposion_ reported uninit memory usages during map_{lookup,delete}_elem. ========== BUG: KMSAN: uninit-value in _ devmap.c:441 [inline] BUG: KMSAN: uninit-value in dev_map_lookup_elem+0xf3/0x170 kernel/bpf/devmap.c:79 bpf/devmap.c:441 [inline] dev_map_lookup_elem+0xf3/0x170 kernel/bpf/devmap.c:796 ____bpf_map_lookup_el bpf_map_lookup_elem+0x5c/0x80 kernel/bpf/helpers.c:38 ___bpf_prog_run+0x13fe/0xe0f0 kernel/bpf/core.c:199 bpf/core.c:2237 ========== The reproducer should be in the interpreter mode. The C reproducer is trying to run (18) r1 = map[id:49] 4: (b7) r8 = 16777216 5: (7b) *(u64 *)(r10 -8) = r8 6: (bf) r2 = r10 7: (07) r2 += -229 ^^^^^^ dev_map_lookup_elem#1543472 11: (95) exit It is due to the "void *key" (r2) passed to the helper. bpf allows unin the right privileges. This patch uses kmsan_unpoison_memory() to mark the stack as initialized. This should addres *key" argument during map_{lookup,delete}_elem.
CVE-2024-42064	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip pipe if the pipe idx not s idx not set properly [how] Add code to skip the pipe that idx not set properly
CVE-2024-42065	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Add a NULL check in xe_ttm_stolen_m the mgr is not NULL.
CVE-2024-42066	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix potential integer overflow in page s >page_alignment to u64 before bit-shifting to prevent overflow when assigning to min_page_size.
CVE-2024-42067	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_rox() into ac set_memory_rox() can fail, leaving memory unprotected. Check return and bail out when bpf_jit_binary_lock_ro()
CVE-2024-42068	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_ro() into acc set_memory_ro() can fail, leaving memory unprotected. Check its return and take it into account as an error.
CVE-2024-42070	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_ store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VAL requires a new helper function to infer the register type from the set datatype so this conditional check can be remo leaked through the registers.

CVE-2024-42076	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_ in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This ca by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrume kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf inclu KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-inf linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 ins instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inl iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/i linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/ socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ____sys_recvmsg+0x18a/0x620 net/socket.c net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_ [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64 include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xc entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inl [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c: skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:65 core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730 net/can/j1939/socket.c:1277 sock_sendmsg_nosec +0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] net/socket.c:2674 x64_sys_call+0xc4b/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 a do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12 of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: sy syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, B
CVE-2024-42077	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transac ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). Th that the IO could be arbitrarily large and can contain arbitrary number of extents. Extent tree manipulations do ofte in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will e all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_met in response to this error. This was actually triggered by one of our customers on a heavily fragmented OCFS2 files transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Hemir - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "Subr ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffff ffffffffc0c88387 [ocfs2] #5 ocfs2_journal_dirty at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ff at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7 #12 do_blockdev_direct_IO at ffffffff8c2bc09f #1 #14 generic_file_direct_write at ffffffff8c1dcf14 #15 __generic_file_write_iter at ffffffff8c1dd07b #16 ocfs2_file_ aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba
CVE-2024-42079	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix NULL pointer dereference in gfs2_log >sd_jdesc to NULL under the log flush lock to provide exclusion against gfs2_log_flush(). In gfs2_log_flush(), che dereferencing it. Otherwise, we could run into a NULL pointer dereference when outstanding glock work races wit run_queue -> do_xmote -> inode_go_sync -> gfs2_log_flush).
CVE-2024-42080	In the Linux kernel, the following vulnerability has been resolved: RDMA/restrack: Fix potential invalid address ac was set to KBUILD_MODNAME in ib_create_cq(), while if the module exited but forgot del this rdma_restrack_e in rdma_restrack_clean() when print the owner of this rdma_restrack_entry. These code is used to help find one for is not needed anymore, so delete them.
CVE-2024-42081	In the Linux kernel, the following vulnerability has been resolved: drm/xe/xe_devcoredump: Check NULL before a 'xe_devcoredump_snapshot *' and 'xe_device *' only if 'coredump' is not NULL. v2 - Fix commit messages. v3 - D v4 - Drop return check for coredump_to_xe. (Jose/Rodrigo) v5 - Modify misleading commit message. (Matt)
CVE-2024-42082	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from __xdp_reg_mem_ __xdp_reg_mem_model(). The warning occurs only if __mem_id_init_hash_table() returns an error. It returns the fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The secon static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with sense in using WARN() to handle this error and it can be safely removed. WARNING: CPU: 0 PID: 5065 at net/co +0x2d9/0x650 net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-g Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+ Trace: xdp_reg_mem_model+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b +0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/ +0x7c/0x90 kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x7 (linuxtesting.org) with syzkaller.

CVE-2024-42084	In the Linux kernel, the following vulnerability has been resolved: ftruncate: pass a signed offset The old ftruncate(extension when called in compat mode on 64-bit architectures. As a result, passing a negative length accidentally s 2GiB and 4GiB. Changing the type of the compat syscall to the signed compat_off_t changes the behavior so it ins the truncate() syscall and the corresponding loff_t based variants are all correct already and do not suffer from this
CVE-2024-42086	In the Linux kernel, the following vulnerability has been resolved: iio: chemical: bme680: Fix overflows in compe compensate functions of the driver that there could be overflows of variables due to bit shifting ops. These implica they were mentioned in log message of Commit 1b3bd8592780 ("iio: chemical: Add support for Bosch BME680 s iio/20180728114028.3c1bbe81@archlinux/
CVE-2024-42087	In the Linux kernel, the following vulnerability has been resolved: drm/panel: ilitek-ili9881c: Fix warning with GP controls the reset GPIO using the non-sleeping gpiod_set_value() function. This complains loudly when the GPIO sleep, use gpiod_set_value_cansleep() to fix the issue.
CVE-2024-42089	In the Linux kernel, the following vulnerability has been resolved: ASoC: fsl-asoc-card: set priv->pdev before usin being used in fsl_asoc_card_audmux_init(). Move this assignment at the start of the probe function, so sub-functio fsl_asoc_card_audmux_init() dereferences priv->pdev to get access to the dev struct, used with dev_err macros. As NULL pointer dereference. Note that if priv->dev is dereferenced before assignment but never used, for example if won't crash probably due to compiler optimisations.
CVE-2024-42090	In the Linux kernel, the following vulnerability has been resolved: pinctrl: fix deadlock in create_pinctrl() when ha pinctrl_maps_mutex is acquired before calling add_setting(). If add_setting() returns -EPROBE_DEFER, create_pi pinctrl_free() attempts to acquire pinctrl_maps_mutex, which is already held by create_pinctrl(), leading to a poten by releasing pinctrl_maps_mutex before calling pinctrl_free(), preventing the deadlock. This bug was discovered a Security Testing (SAST) by Synopsys, Inc.
CVE-2024-42091	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Check pat.ops before dumping PAT set running on brand new platform or when running as a VF. While the former is unlikely, the latter is valid (future) us will try to dump PAT settings by debugfs. It's better to check pointer to pat.ops instead of specific .dump hook, as every .ops variant.
CVE-2024-42092	In the Linux kernel, the following vulnerability has been resolved: gpio: davinci: Validate the obtained number of I from Device Tree. In case of broken DT due to any error this value can be any. Without this value validation there access in davinci_gpio_probe(). Validate the obtained nirq value so that it won't exceed the maximum number of II Center (linuxtesting.org) with SVACE.
CVE-2024-42093	In the Linux kernel, the following vulnerability has been resolved: net/dpaa2: Avoid explicit cpumask var allocatio CONFIG_CPUMASK_OFFSTACK=y kernel, explicit allocation of cpumask variable on stack is not recommende overflow. Instead, kernel code should always use *cpumask_var API(s) to allocate cpumask var in config-neutral v CONFIG_CPUMASK_OFFSTACK. Use *cpumask_var API(s) to address it.
CVE-2024-42094	In the Linux kernel, the following vulnerability has been resolved: net/iucv: Avoid explicit cpumask var allocation CONFIG_CPUMASK_OFFSTACK=y kernel, explicit allocation of cpumask variable on stack is not recommende overflow. Instead, kernel code should always use *cpumask_var API(s) to allocate cpumask var in config-neutral v CONFIG_CPUMASK_OFFSTACK. Use *cpumask_var API(s) to address it.
CVE-2024-42095	In the Linux kernel, the following vulnerability has been resolved: serial: 8250_omap: Implementation of Errata i2 timeout can be triggered, if this Erroneous interrupt is not cleared then it may leads to storm of interrupts, therefore www.ti.com/lit/pdf/sprz536 page 23
CVE-2024-42096	In the Linux kernel, the following vulnerability has been resolved: x86: stop playing stack games in profile_pc() Th timer-based profiling, which isn't really all that relevant any more to begin with, but it also ends up making assump necessarily valid. Basically, the code tries to account the time spent in spinlocks to the caller rather than the spinlo not worth the code complexity or the KASAN warnings when no serious profiling is done using timers anyway the stack layout that is only true in the simplest of cases. We've lost the comment at some point (I think when the 32-bi to say: Assume the lock function has either no stack frame or a copy of eflags from PUSHF. which explains why it off the stack pointer and then takes a minimal look at the values to just check if they might be eflags or the return p unlike kernel addresses but that basic stack layout assumption assumes that there isn't any lock debugging etc going a stack frame. It causes KASAN unhappiness reported for years by syzkaller [1] and others [2]. With no real practi the code. Just for historical interest, here's some background commits relating to this code from 2006: 0cb91a2293 during profiling for !FP kernels") 31679f38d886 ("Simplify profile_pc on x86-64") and a code unification from 20 profile_pc") but the basics of this thing actually goes back to before the git tree.
CVE-2024-42097	In the Linux kernel, the following vulnerability has been resolved: ALSA: emux: improve patch ioctl data validatio skipping over the main info block match that in load_guspatch(). In load_guspatch(), add checking that the specifie data, like load_data() already did.
CVE-2024-42098	In the Linux kernel, the following vulnerability has been resolved: crypto: ecdh - explicitly zeroize private_key pri parameter passed in by the caller (if present), or alternatively a newly generated private key. However, it is possibl generated key) which is shorter than the previous key. In that scenario, some key material from the previous key w is to explicitly zeroize the entire private_key array first. Note that this patch slightly changes the behavior of this fu failed, the old private_key would remain. Now, the private_key is always zeroized. This behavior is consistent with ecc_is_key_valid fails.

CVE-2024-42101	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau: fix null pointer dereference in nou nouveau_connector_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead t failure of drm_mode_duplicate(). Add a check to avoid npd.
CVE-2024-42102	In the Linux kernel, the following vulnerability has been resolved: Revert "mm/writeback: fix possible divide-by-z "mm: Avoid possible overflows in dirty throttling". Dirty throttling logic assumes dirty limits in page units fit into true (see patch 2/2 for more details). This patch (of 2): This reverts commit 9319b647902cbd5cc884ac08a8a6d54c ways. Firstly, the removed (u64) cast from the multiplication will introduce a multiplication overflow on 32-bit arc is actually common - the default settings with 4GB of RAM will trigger this). Secondly, the div64_u64() is unneces div64_ul() in case we want to be safe & cheap. Thirdly, if dirty thresholds are larger than 1<<32 pages, then dirty b spectacular ways anyway so trying to fix one possible overflow is just moot.
CVE-2024-42104	In the Linux kernel, the following vulnerability has been resolved: nilfs2: add missing check for inode numbers on mounting and unmounting a specific pattern of corrupted nilfs2 filesystem images causes a use-after-free of metada lru_add_fn(). As Jan Kara pointed out, this is because the link count of a metadata file gets corrupted to 0, and nilfs tries to delete that inode (ifile inode in this case). The inconsistency occurs because directories containing the inode not be visible in the namespace are read without checking. Fix this issue by treating the inode numbers of these inte when reading directory folios/pages. Also thanks to Hillf Danton and Matthew Wilcox for their initial mm-layer an
CVE-2024-42105	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix inode number range checks Patch seri to reserved inodes". This series fixes one use-after-free issue reported by syzbot, caused by nilfs2's internal inode b corrupted filesystem, and a couple of flaws that cause problems if the starting number of non-reserved inodes writt (or corruptly) changed from its default value. This patch (of 3): In the current implementation of nilfs2, "nilfs->ns_ reserved inode number, is read from the superblock, but its lower limit is not checked. As a result, if a number that of reserved inodes such as the root directory or metadata files is set in the super block parameter, the inode number NILFS_VALID_INODE) will not function properly. In addition, these test macros use left bit-shift calculations usi via the BIT macro, but the result of a shift calculation that exceeds the bit width of an integer is undefined in the C a large value other than the default value NILFS_USER_INO (=11), the macros may potentially malfunction deper by checking the lower bound of "nilfs->ns_first_ino" and by preventing bit shifts equal to or greater than the NILF test macros. Also, change the type of "ns_first_ino" from signed integer to unsigned integer to avoid the need for ty bound check introduced this time.
CVE-2024-42106	In the Linux kernel, the following vulnerability has been resolved: inet_diag: Initialize pad field in struct inet_diag value access in raw_lookup() [1]. Diag for raw sockets uses the pad field in struct inet_diag_req_v2 for the underly to the sdiag_raw_protocol field in struct inet_diag_req_raw. inet_diag_get_exact_compat() converts inet_diag_req the pad field uninitialized. So the issue occurs when raw_lookup() accesses the sdiag_raw_protocol field. Fix this b inet_diag_get_exact_compat(). Also, do the same fix in inet_diag_dump_compat() to avoid the similar issue in the in raw_lookup net/ipv4/raw_diag.c:49 [inline] BUG: KMSAN: uninit-value in raw_sock_get+0x657/0x800 net/ipv raw_diag.c:49 [inline] raw_sock_get+0x657/0x800 net/ipv4/raw_diag.c:71 raw_diag_dump_one+0xa1/0x660 net/i +0x7d9/0x980 inet_diag_get_exact_compat net/ipv4/inet_diag.c:1404 [inline] inet_diag_rcv_msg_compat+0x469/ sock_diag_rcv_msg+0x23d/0x740 net/core/sock_diag.c:282 netlink_rcv_skb+0x537/0x670 net/netlink/af_netlink.c net/core/sock_diag.c:297 netlink_unicast_kernel net/netlink/af_netlink.c:1335 [inline] netlink_unicast+0xe74/0x12 netlink_sendmsg+0x10c6/0x1260 net/netlink/af_netlink.c:1905 sock_sendmsg_nosec net/socket.c:730 [inline] __s socket.c:745 ____sys_sendmsg+0x7f0/0xb70 net/socket.c:2585 ___sys_sendmsg+0x271/0x3b0 net/socket.c:2639 __do_sys_sendmsg net/socket.c:2677 [inline] __se_sys_sendmsg net/socket.c:2675 [inline] __x64_sys_sendmsg+0 +0x135e/0x3ce0 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [in entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was stored to memory at: raw_sock_g raw_diag_dump_one+0xa1/0x660 net/ipv4/raw_diag.c:99 inet_diag_cmd_exact+0x7d9/0x980 inet_diag_get_exac [inline] inet_diag_rcv_msg_compat+0x469/0x530 net/ipv4/inet_diag.c:1426 sock_diag_rcv_msg+0x23d/0x740 ne +0x537/0x670 net/netlink/af_netlink.c:2564 sock_diag_rcv+0x35/0x40 net/core/sock_diag.c:297 netlink_unicast_k netlink_unicast+0xe74/0x1240 net/netlink/af_netlink.c:1361 netlink_sendmsg+0x10c6/0x1260 net/netlink/af_netli socket.c:730 [inline] __sock_sendmsg+0x332/0x3d0 net/socket.c:745 ____sys_sendmsg+0x7f0/0xb70 net/socket.c net/socket.c:2639 __sys_sendmsg net/socket.c:2668 [inline] __do_sys_sendmsg net/socket.c:2677 [inline] __se_sy __x64_sys_sendmsg+0x27e/0x4a0 net/socket.c:2675 x64_sys_call+0x135e/0x3ce0 arch/x86/include/generated/asm arch/x86/entry/common.c:52 [inline] do_syscall_64+0xd9/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_6 variable req.i created at: inet_diag_get_exact_compat net/ipv4/inet_diag.c:1396 [inline] inet_diag_rcv_msg_compa sock_diag_rcv_msg+0x23d/0x740 net/core/sock_diag.c:282 CPU: 1 PID: 8888 Comm: syz-executor.6 Not tainted Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-2.fc40 04/01/2014

CVE-2024-42110	In the Linux kernel, the following vulnerability has been resolved: net: ntb_netdev: Move ntb_netdev_rx_handler() The following is emitted when using idxd (DSA) dmanegine as the data mover for ntb_transport that ntb_netdev us smp_processor_id() in preemptible [00000000] code: irq/52-idxd-por/14526 [74412.556784] caller is netif_rx_inte CPU: 6 PID: 14526 Comm: irq/52-idxd-por Not tainted 6.9.5 #5 [74412.569870] Hardware name: Intel Corporatio EGSDCRB1.E9I.1752.P05.2402080856 02/08/2024 [74412.581699] Call Trace: [74412.584514] <TASK> [74412 [74412.591129] check_preemption_disabled+0xc8/0xf0 [74412.596374] netif_rx_internal+0x42/0x130 [74412.60 ntb_netdev_rx_handler+0x66/0x150 [ntb_netdev] [74412.610985] ntb_complete_rxc+0xed/0x140 [ntb_transport] +0x53/0x80 [ntb_transport] [74412.623332] idxd_dma_complete_txd+0xe3/0x160 [idxd] [74412.628963] idxd_w irq_thread_fn+0x21/0x60 [74412.638134] ? irq_thread+0xa8/0x290 [74412.642218] irq_thread+0x1a0/0x290 [744 +0x10/0x10 [74412.651071] ? __pfx_irq_thread_dtor+0x10/0x10 [74412.656117] ? __pfx_irq_thread+0x10/0x10 [74412.664384] ? __pfx_kthread+0x10/0x10 [74412.668639] ret_from_fork+0x31/0x50 [74412.672716] ? __pfx_ ret_from_fork_asm+0x1a/0x30 [74412.681457] </TASK> The cause is due to the idxd driver interrupt completion threaded handler is not hard or soft interrupt context. However __netif_rx() can only be called from interrupt conte to allow completion via normal context for dmaengine drivers that utilize threaded irq handling. While the followir __netif_rx(), baebdf48c360 ("net: dev: Makes sure netif_rx() can be invoked in any context."), the change should've precedes this fix should've been using netif_rx_ni() or netif_rx_any_context().
CVE-2024-42114	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: restrict NL80211_ATTR_TXQ_ trigger softlockups, setting NL80211_ATTR_TXQ_QUANTUM to 2^31. We had a similar issue in sch_fq, fixed v fq: do not accept silly TCA_FQ_QUANTUM") watchdog: BUG: soft lockup - CPU#1 stuck for 26s! [kworker/1:0: 131135 hardirqs last enabled at (131134): [<ffff80008ae8778c>] __exit_to_kernel_mode arch/arm64/kernel/entry- enabled at (131134): [<ffff80008ae8778c>] exit_to_kernel_mode+0xdc/0x10c arch/arm64/kernel/entry-common.c [<ffff80008ae85378>] __el1_irq arch/arm64/kernel/entry-common.c:533 [inline] hardirqs last disabled at (131135 +0x24/0x68 arch/arm64/kernel/entry-common.c:551 softirqs last enabled at (125892): [<ffff80008907e82c>] neigh [inline] softirqs last enabled at (125892): [<ffff80008907e82c>] neigh_resolve_output+0x268/0x658 net/core/neigh (125896): [<ffff80008904166c>] local_bh_disable+0x10/0x34 include/linux/bottom_half.h:19 CPU: 1 PID: 24 Co rc7-syzkaller-gfda5695d692c #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS mld mld_ifc_work pstate: 80400005 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __list_del includ __list_del_entry include/linux/list.h:218 [inline] pc : list_move_tail include/linux/list.h:310 [inline] pc : fq_tin_deq ieee80211_tx_dequeue+0x6b8/0x3b4c net/mac80211/tx.c:3854 lr : __list_del_entry include/linux/list.h:218 [inline [inline] lr : fq_tin_dequeue include/net/fq_impl.h:112 [inline] lr : ieee80211_tx_dequeue+0x67c/0x3b4c net/mac80 x29: ffff800093d36a60 x28: ffff800093d36960 x27: dfff800000000000 x26: ffff0000d800ad50 x25: ffff0000d800a x23: ffff0000e0032468 x22: ffff0000e00324d4 x21: ffff0000d800abf0 x20: ffff0000d800abf8 x19: ffff0000d800ab 000000000000d476 x16: ffff8000805519dc x15: ffff7000127a6cc8 x14: 1ffff000127a6cc8 x13: 00000000000000 x10: 0000000000ff0100 x9 : 0000000000000000 x8 : 0000000000000000 x7 : 0000000000000000 x6 : 00000000 0000000000000008 x3 : ffff80008034c7fc x2 : ffff0000e0032468 x1 : 00000000da0e46b8 x0 : ffff0000e0032470 [inline] __list_del_entry include/linux/list.h:218 [inline] list_move_tail include/linux/list.h:310 [inline] fq_tin_dequ ieee80211_tx_dequeue+0x6b8/0x3b4c net/mac80211/tx.c:3854 wake_tx_push_queue net/mac80211/util.c:294 [inl +0x118/0x274 net/mac80211/util.c:315 drv_wake_tx_queue net/mac80211/driver-ops.h:1350 [inline] schedule_an [inline] ieee80211_queue_skb+0x18e8/0x2244 net/mac80211/tx.c:1664 ieee80211_tx+0x260/0x400 net/mac80211 net/mac80211/tx.c:2062 __ieee80211_subif_start_xmit+0xab8/0x122c net/mac80211/tx.c:4338 ieee80211_subif_s tx.c:4532 __netdev_start_xmit include/linux/netdevice.h:4903 [inline] netdev_start_xmit include/linux/netdevice.h [inline] dev_hard_start_xmit+0x27c/0x938 net/core/dev.c:3547 __dev_queue_xmit+0x1678/0x33fc net/core/dev.c: netdevice.h:3091 [inline] neigh_resolve_output+0x558/0x658 net/core/neighbour.c:1563 neigh_output include/net/ truncated---
CVE-2024-42115	In the Linux kernel, the following vulnerability has been resolved: jffs2: Fix potential illegal address access in jffs2 jffs2 file system,the following abnormal printouts were found: [2430.649000] Unable to handle kernel paging requ [2430.649622] Mem abort info: [2430.649829] ESR = 0x96000004 [2430.650115] EC = 0x25: DABT (current E FnV = 0 [2430.650795] EA = 0, S1PTW = 0 [2430.651032] FSC = 0x04: level 0 translation fault [2430.651446] = 0x00000004 [2430.652001] CM = 0, WnR = 0 [2430.652558] [0069696969696948] address between user and k error: Oops: 96000004 [#1] PREEMPT SMP [2430.654512] CPU: 2 PID: 20919 Comm: cat Not tainted 5.15.25-g name: linux,dummy-virt (DT) [2430.655517] pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYP [2430.656630] lr : jffs2_free_inode+0x24/0x48 [2430.657051] sp : ffff800009eebd10 [2430.657355] x29: ffff80 0000000000000000 [2430.658327] x26: ffff000038f09d80 x25: 0080000000000000 x24: ffff800009d38000 [243 ffff000038f09d80 x21: ffff8000084f0d14 [2430.659434] x20: ffff0000bf9a6ac0 x19: 0169696969696940 x18: 00 ffff8000b6506000 x16: ffff800009eec000 x15: 0000000000004000 [2430.660637] x14: 0000000000000000 x13: [2430.661345] x11: 0004000800000000 x10: 0000000000000001 x9 : ffff8000084f0d14 [2430.662025] x8 : ffff0 x6 : 0000000003470302 [2430.662695] x5 : ffff00002e41dcc0 x4 : ffff0000bf9aa3b0 x3 : 0000000003470342 [24 x1 : ffff8000084f0d14 x0 : fffffc0000000000 [2430.664217] Call trace: [2430.664528] kfree+0x78/0x348 [2430. [2430.665233] i_callback+0x24/0x50 [2430.665528] rcu_do_batch+0x1ac/0x448 [2430.665892] rcu_core+0x28 +0x18/0x28 [2430.666473] __do_softirq+0x138/0x3cc [2430.666781] irq_exit+0xf0/0x110 [2430.667065] handl gic_handle_irq+0xac/0xe8 [2430.667739] call_on_irq_stack+0x28/0x54 The parameter passed to kfree was 5a5a5 the jffs_inode_info structure. It was found that all variables in the jffs_inode_info structure were 5a5a5a5a, except these variables are not initialized because they were set to 5a5a5a5a during memory testing, which is meant to dete is initialized in the function jffs2_i_init_once, while other members are initialized in the function jffs2_init_inode_ is called after iget_locked, but in the iget_locked function, the destroy_inode process is triggered, which releases th member of the inode is not initialized.In concurrent high pressure scenarios, iget_locked may enter the destroy_ino destroy_inode functionality of jffs2 only releases the target, the fix method is to set target to NULL in jffs2_i_init_

CVE-2024-42116	In the Linux kernel, the following vulnerability has been resolved: igc: fix a log entry using uninitialized netdev Du [5.133667] igc 0000:01:00.0 (unnamed net_device) (uninitialized): PHC added ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ is called very early, even before register_netdev() has been called. So the netdev_info() call works on a partially un igc_ptp_init() after register_netdev(), right after the media autosense check, just as in igb. Add a comment, just as i [5.200987] igc 0000:01:00.0 eth0: PHC added
CVE-2024-42117	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: ASSERT when failing to find find_disp_cfg_idx_by_plane_id and find_disp_cfg_idx_by_stream_id returns an array index and they return -1 whe number. [HOW] When this happens, call ASSERT(), and return a positive number (which is fewer than callers' arr 2 NEGATIVE_RETURNS issues reported by Coverity.
CVE-2024-42118	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Do not return negative stream resource_stream_to_stream_idx returns an array index and it return -1 when not found; however, -1 is not a valid a happens, call ASSERT(), and return a zero instead. This fixes an OVERRUN and an NEGATIVE_RETURNS issu
CVE-2024-42119	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip finding free audio for un ENGINE_ID_UNKNOWN = -1 and can not be used as an array index. Plus, it also means it is uninitialized and do return NULL. This fixes 2 OVERRUN issues reported by Coverity.
CVE-2024-42120	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check pipe offset before setti so checking its index before accessing the array. This fixes an OVERRUN issue reported by Coverity.
CVE-2024-42121	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check index msg_id before re array index and it cannot be a negative value, and therefore cannot be equal to MOD_HDCP_MESSAGE_ID_INV valid before reading and setting. This fixes 4 OVERRUN issues reported by Coverity.
CVE-2024-42122	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add NULL pointer check for of kzalloc before using it.
CVE-2024-42123	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix double free err_addr pointer w amdgpu_umc_bad_page_polling_timeout, the amdgpu_umc_handle_bad_pages will be run many times so that dou the err_addr to NULL to avoid the warnings.
CVE-2024-42124	In the Linux kernel, the following vulnerability has been resolved: scsi: qedf: Make qedf_execute_tmf() non-preem preemptible code in qedf_execute_tmf90. This results in BUG_ON() when running an RT kernel. [659.343280] B [00000000] code: sg_reset/3646 [659.343282] caller is qedf_execute_tmf+0x8b/0x360 [qedf]
CVE-2024-42125	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: fw: scan offload prohibit all 6 GHz policy via BIOS to block uses of 6 GHz. In this case, 6 GHz sband will be NULL even if it is WiFi 7 chip. So, add
CVE-2024-42126	In the Linux kernel, the following vulnerability has been resolved: powerpc: Avoid nmi_enter/nmi_exit in real moc per cpu variables which can lead to kernel crash when invoked during real mode interrupt handling (e.g. early HMI comes from vmalloc area. Early HMI/MCE handlers are called through DEFINE_INTERRUPT_HANDLER_NMI calls. We don't see any issue when percpu allocation is from the embedded first chunk. However with CONFIG_NI enabled there are chances where percpu allocation can come from the vmalloc area. With kernel command line "pe percpu allocation to come from vmalloc area and can see kernel crash in machine_check_early: [1.215714] NIP [c +0x24/0x110 [1.215717] LR [c0000000000461a0] machine_check_early+0xf0/0x2c0 [1.215719] --- interrupt: 20 [0000000000000000] 0x0 (unreliable) [1.215722] [c000000fffd731b0] [0000000000000000] 0x0 [1.215724] [c00 machine_check_early_common+0x134/0x1f8 Fix this by avoiding use of nmi_enter()/nmi_exit() in real mode if pe
CVE-2024-42127	In the Linux kernel, the following vulnerability has been resolved: drm/lima: fix shared irq handling on driver remo interrupt handlers must be prepared to be called at any time. At driver removal time, the clocks are disabled early a very end of the remove process due to the devm usage. This is potentially a bug as the interrupts access device regi crash can be triggered by removing the driver in a kernel with CONFIG_DEBUG_SHIRQ enabled. This patch free callback so that the handlers are already unregistered by the time we fully disable clocks.
CVE-2024-42128	In the Linux kernel, the following vulnerability has been resolved: leds: an30259a: Use devm_mutex_init() for mut registered using devm_led_classdev_register() so they are automatically unregistered after module's remove() is do led_set_brightness() to turn off the LEDs and that callback uses mutex which was destroyed already in module's re
CVE-2024-42129	In the Linux kernel, the following vulnerability has been resolved: leds: mlxreg: Use devm_mutex_init() for mutex registered using devm_led_classdev_register() so they are automatically unregistered after module's remove() is do led_set_brightness() to turn off the LEDs and that callback uses mutex which was destroyed already in module's re
CVE-2024-42130	In the Linux kernel, the following vulnerability has been resolved: nfc/nci: Add the inconsistency check between th &(0x7f0000000740)=ANY=[@ANYBLOB="610501"], 0xf) Syzbot constructed a write() call with a data length o passed too little data to meet the basic requirements of the function nci_rf_intf_activated_ntf_packet(). Therefore, i length and count value to avoid problems caused by inconsistent data length and count.

CVE-2024-42131	In the Linux kernel, the following vulnerability has been resolved: mm: avoid overflows in dirty throttling logic Th assumptions that dirty limits in PAGE_SIZE units fit into 32-bit (so that various multiplications fit into 64-bits). If overflows, possible divisions by 0 etc. Fix these problems by never allowing so large dirty limits as they have dubi dirty_background_bytes interfaces we can just refuse to set so large limits. For dirty_ratio / dirty_background_ratio computed from the amount of available memory which can change due to memory hotplug etc. So when convertin we just don't allow the result to exceed UINT_MAX. This is root-only triggerable problem which occurs when the
CVE-2024-42134	In the Linux kernel, the following vulnerability has been resolved: virtio-pci: Check if is_avq is NULL [bug] In the vp_dev->is_avq is involved to determine whether it is admin virtqueue, but this function vp_dev->is_avq may be e does not assign a value to vp_dev->is_avq. [fix] Check whether it is vp_dev->is_avq before use. [test] Test with vi following command would crash the guest system After applying the patch, everything seems to be working fine.
CVE-2024-42135	In the Linux kernel, the following vulnerability has been resolved: vhost_task: Handle SIGKILL by flushing work device is closed, this has us handle SIGKILL by: 1. marking the worker as killed so we no longer try to use it with setting the virtqueue to worker mapping so no new works are queued. 3. running all the exiting works.
CVE-2024-42136	In the Linux kernel, the following vulnerability has been resolved: cdrom: rearrange last_media_change check to a syzkaller with the newly reintroduced signed integer wrap sanitizer we encounter this splat: [366.015950] UBSAN cdrom/cdrom.c:2361:33 [366.021089] -9223372036854775808 - 346321 cannot be represented in type '__s64' (ak executor.4 is using a deprecated SCSI ioctl, please convert it to SG_IO [366.027502] CPU: 5 PID: 28472 Comm: gb3ef86b5a957 #1 [366.027512] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debia Call Trace: [366.027523] <TASK> [366.027533] dump_stack_lvl+0x93/0xd0 [366.027899] handle_overflow+0x multi_count 32 ignored [366.043924] cdrom_ioctl+0x2c3f/0x2d10 [366.063932] ? __pm_runtime_resume+0xe6/ +0x15d/0x1d0 [366.074624] ? __pfx_sr_block_ioctl+0x10/0x10 [366.077642] blkdev_ioctl+0x419/0x500 [366.0 Historically, the signed integer overflow sanitizer did not work in the kernel due to its interaction with `-fwrapv` bu newest version of Clang. It was re-enabled in the kernel with Commit 557f8c582a9ba8ab ("ubsan: Reintroduce sig check to not perform any arithmetic, thus not tripping the sanitizer.
CVE-2024-42137	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: qca: Fix BT enable failure again for 272970be3dab ("Bluetooth: hci_qca: Fix driver shutdown on closed serdev") will cause below regression issue: BT boot -> enable BT -> disable BT -> warm reboot -> BT enable failure if property enable-gpios is not configured wi is to fix a use-after-free issue within qca_serdev_shutdown() by adding condition to avoid the serdev is flushed or regression issue regarding above steps since the VSC is not sent to reset controller during warm reboot. Fixed by se qca_serdev_shutdown() once BT was ever enabled, and the use-after-free issue is also fixed by this change since th or wrote. Verified by the reported machine Dell XPS 13 9310 laptop over below two kernel commits: commit e00f coredump implementation for QCA") of bluetooth-next tree. commit b23d98d46d28 ("Bluetooth: btusb: Fix trigge linus mainline tree.
CVE-2024-42143	In the Linux kernel, the following vulnerability has been resolved: orangefs: fix out-of-bounds fsid access Arnd Be "orangefs_statfs() copies two consecutive fields of the superblock into the statfs structure, which triggers a warning Kara suggested an alternate way to do the patch to make it more readable. I ran both ideas through xfstests and both suggestion.
CVE-2024-42144	In the Linux kernel, the following vulnerability has been resolved: thermal/drivers/mediatek/lvts_thermal: Check N not NULL before using it.
CVE-2024-42145	In the Linux kernel, the following vulnerability has been resolved: IB/core: Implement a limit on UMAD receive L maintains received MAD packets in an unbounded list, poses a risk of uncontrolled growth. As user-space applicati of extraction may not match the rate of incoming packets, leading to potential list overflow. To address this, we int considering typical scenarios, such as OpenSM processing, which can handle approximately 100k packets per seco packets, we set the list size limit to 200k. Packets received beyond this limit are dropped, assuming they are likely user-space. Notably, packets queued on the receive list due to reasons like timed-out sends are preserved even whe
CVE-2024-42146	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Add outer runtime_pm protection to xe doing any memory access should get their own runtime_pm outer references since they don't use the standard drive from the same driver. Found by pre-merge CI on adding WARN calls for unprotected inner callers: <6> [318.6397 xe_test_dmabuf_import_same_driver <4> [318.639957] ------------[cut here]------------ <4> [318.639967] xe 0000 protection <4> [318.640049] WARNING: CPU: 117 PID: 3832 at drivers/gpu/drm/xe/xe_pm.c:533 xe_pm_runtim
CVE-2024-42147	In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/debugfs - Fix debugfs uninit pr the debugfs failure does not stop the probe. When debugfs initialization fails, jumping to the error branch will also operation. As a result, it may be released repeatedly during the regs uninit process. Therefore, the null check needs

CVE-2024-42148	In the Linux kernel, the following vulnerability has been resolved: bnx2x: Fix multiple UBSAN array-index-out-of when using a system with 32 physical cpu cores or more, or when the user defines a number of Ethernet queues gre using the num_queues module parameter. Currently there is a read/write out of bounds that occurs on the array "str the "bnx2x_fw_stats_req" struct in "drivers/net/ethernet/broadcom/bnx2x/bnx2x.h". Looking at the definition of th struct stats_query_entry query[FP_SB_MAX_E1x+ BNX2X_FIRST_QUEUE_QUERY_IDX]; FP_SB_MAX_E1 fast path interrupts and has a value of 16, while BNX2X_FIRST_QUEUE_QUERY_IDX has a value of 3 meaning accesses to "struct stats_query_entry query" are offset-ted by BNX2X_FIRST_QUEUE_QUERY_IDX, that means should not exceed FP_SB_MAX_E1x (16). However one of these queues is reserved for FCOE and thus the numbe [FP_SB_MAX_E1x -1] (15) if FCOE is enabled or [FP_SB_MAX_E1x] (16) if it is not. This is also described in a ethernet/broadcom/bnx2x/bnx2x.h just above the Macro definition of FP_SB_MAX_E1x. Below is the part of this * The total number of L2 queues, MSIX vectors and HW contexts (CIDs) is * control by the number of fast-path st FW). Each fast-path status block (FP-SB) aka non-default * status block represents an independent interrupts conte queue. However special L2 queues such * as the FCoE queue do not require a FP-SB and other components like * number of possible L2 queues * * If the maximum number of FP-SB available is X then: * a. If CNIC is supported of * regular L2 queues is Y=X-1 * b. In MF mode the actual number of L2 queues is Y= (X-1/MF_factor) * c. If th number of L2 queues * is Y+1 * d. The number of irqs (MSIX vectors) is either Y+1 (one extra for * slow-path int additional * FP interrupt context for the CNIC). * e. The number of HW context (CID count) is always X or X+1 if the FCoE L2 queue is always X. */ However this driver also supports NICs that use the E2 controller which can ha represented by FP_SB_MAX_E2. Looking at the commits when the E2 support was added, it was originally using ("bnx2x: Add 57712 support"). Back then FP_SB_MAX_E2 was set to 16 the same as E1x. However the driver wa E2 instead of having it be limited to the capabilities of the E1x. But as far as we can tell, the array "stats_query_ent SB available to the E1x cards as part of an oversight when the driver was updated to take full advantage of the E2, greater queue size supported by E2 NICs, it causes the UBSAN warnings seen in the stack traces below. This patch query" array by replacing FP_SB_MAX_E1x with FP_SB_MAX_E2 to be large enough to handle both types of NI of-bounds in drivers/net/ethernet/broadcom/bnx2x/bnx2x_stats.c:1529:11 index 20 is out of range for type 'stats_qu systemd-network Not tainted 6.9.0-060900rc7-generic #202405052133 Hardware name: HP ProLiant DL360 Gen9
CVE-2024-42151	In the Linux kernel, the following vulnerability has been resolved: bpf: mark bpf_dummy_struct_ops.test_1 parame dummy_init_ret_value passes NULL as the first parameter of the test_1() function. Mark this parameter as nullable Otherwise, NULL check in the test_1() code: SEC("struct_ops/test_1") int BPF_PROG(test_1, struct bpf_dummy_ access state ... } Might be removed by verifier, thus triggering NULL pointer dereference under certain conditions.
CVE-2024-42152	In the Linux kernel, the following vulnerability has been resolved: nvmet: fix a possible leak when destroy a ctrl du we capture sq->ctrl early and if it is non-NULL we know that a ctrl was allocated (in the admin connect request har clear ctrl->sqs and sq->ctrl (for nvme-loop primarily), and drop the final reference on the ctrl. However, a small wi starts (as a result of the client giving up and disconnecting) concurrently with the nvme admin connect cmd (which kill_and_confirm of sq->ref (i.e. the admin connect managed to get an sq live reference). In this case, sq->ctrl was a local variable in nvmet_sq_destroy. This prevented the final reference drop on the ctrl. Solve this by re-capturing completed, where for sure sq->ctrl reference is final, and move forward based on that. This issue was observed in a multiple ctrls simoutanuosly, creating a delay in allocating a ctrl leading up to this race window.
CVE-2024-42153	In the Linux kernel, the following vulnerability has been resolved: i2c: pnx: Fix potential deadlock warning from d del_timer_sync() is called in an interrupt context it throws a warning because of potential deadlock. The timer is us after a timeout so replacing the call with wait_for_completion_timeout() allows to remove the problematic timer ar
CVE-2024-42154	In the Linux kernel, the following vulnerability has been resolved: tcp_metrics: validate source addr length I don't s TCP_METRICS_ATTR_SADDR_IPV4 is at least 4 bytes long, and the policy doesn't have an entry for this attribu manually validated).
CVE-2024-42155	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe copies of protected- and secure protected- nor secure-keys is accessible, this key material should only be visible to the calling process. So wipe all stack, even in case of an error.
CVE-2024-42156	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe copies of clear-key structures for all IOCTLs, which convert a clear-key into a protected- or secure-key.
CVE-2024-42157	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe sensitive data on failure Wipe copy_to_user() fails.
CVE-2024-42158	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Use kfree_sensitive() to fix Coccinel and kfree() with kfree_sensitive() to fix warnings reported by Coccinelle: WARNING opportunity for kfree_sensiti opportunity for kfree_sensitive/kvfree_sensitive (line 1643) WARNING opportunity for kfree_sensitive/kvfree_sen
CVE-2024-42159	In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Sanitise num_phys Information is larger then size of this field shouldn't be allowed.
CVE-2024-42160	In the Linux kernel, the following vulnerability has been resolved: f2fs: check validation of fault attrs in f2fs_build fault attrs in parse_options(), let's fix to add check condition in f2fs_build_fault_attr(). - Use f2fs_build_fault_attr()

CVE-2024-42161	In the Linux kernel, the following vulnerability has been resolved: bpf: Avoid uninitialized value in BPF_CORE_R Use a default branch in the switch statement to initialize `val'.] GCC warns that `val' may be used uninitialized in th defined in bpf_core_read.h as: [...] unsigned long long val; \ [...] \ switch (__CORE_RELO(s, field, BYTE_SIZE)) break; \ case 2: val = *(const unsigned short *)p; break; \ case 4: val = *(const unsigned int *)p; break; \ case 8: val \ [...] val; \ } \ This patch adds a default entry in the switch statement that sets `val' to zero in order to avoid the war __builtin_preserve_field_info returns unexpected values for BPF_FIELD_BYTE_SIZE. Tested in bpf-next master.
CVE-2024-42162	In the Linux kernel, the following vulnerability has been resolved: gve: Account for stopped queues when reading I NIC might send us stats for a subset of queues. Without this change, gve_get_ethtool_stats might make an invalid a
CVE-2024-42223	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: tda10048: Fix integer ove can overflow a 32 bit integer when multiplied by pll_mfactor. Create a new 64 bit variable to hold the calculations.
CVE-2024-42224	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mv88e6xxx: Correct check for empty l mv88e6xxx: Support multiple MDIO busses") mv88e6xxx_default_mdio_bus() has checked that the return value o to be intended to guard against the list chip->mdios being empty. However, it is not the correct check as the implen return NULL for empty lists. Instead, use list_first_entry_or_null() which does return NULL if the list is empty. Fl
CVE-2024-42225	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: replace skb_put with skb_put_zero A
CVE-2024-42226	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: prevent potential failure in handle_tx_ Some transfer events don't always point to a TRB, and consequently don't have a endpoint ring. In these cases, func because if 'ep->skip' is set, the pointer to the endpoint ring is used. To prevent a potential failure and make the code code for a Transfer event without TRBs.
CVE-2024-42227	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix overlapping copy within c &mode_lib->mp.Watermark and &locals->Watermark are the same address. memcpy may lead to unexpected beha
CVE-2024-42228	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Using uninitialized value *size wh the size before calling amdgpu_vce_cs_reloc, such as case 0x03000001. V2: To really improve the handling we wo 0xffffffff.(Christian)
CVE-2024-42229	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use variables temporarily holding cryptographic information should be zeroized once they are no longer needed. Accor buffers that previously held the private key.
CVE-2024-42230	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix scv instruction crash with I (reloc_on_exc), required for scv instruction support, before other CPUs have been shut down. This means they can disabled, which causes an interrupt at an unexpected entry location that crashes the kernel. Change the kexec seque have been brought down. As a refresher, the real-mode scv interrupt vector is 0x17000, and the fixed-location head implementing such high addresses so it was just decided not to support that interrupt at all.
CVE-2024-4317	Missing authorization in PostgreSQL built-in views pg_stats_ext and pg_stats_ext_exprs allows an unprivileged da and other statistics from CREATE STATISTICS commands of other users. The most common values may reveal c not otherwise read or results of functions they cannot execute. Installing an unaffected version only fixes fresh Post are created with the initdb utility after installing that version. Current PostgreSQL installations will remain vulnera the release notes. Within major versions 14-16, minor versions before PostgreSQL 16.3, 15.7, and 14.12 are affecte unaffected.
DSA-5349-1	gnutls28 - security update
DSA-5402-1	linux - security update
DSA-5453-1	linux - security update
DSA-5461-1	linux - security update
DSA-5475-1	linux - security update
DSA-5480-1	linux - security update
DSA-5523-1	curl - security update
DSA-5523-1	curl - security update
DSA-5570-1	nghttp2 - security update
DSA-5587-1	curl - security update
DSA-5587-1	curl - security update
DSA-5594-1	linux - security update
DSA-5681-1	linux - security update
DSA-5703-1	linux - security update

DSA-5730-1	linux - security update
GHSA-9h6g-pr28-7cqp	### Summary A ReDoS vulnerability occurs when nodemailer tries to parse img files with the parameter `attachDa event loop. Another flaw was found when nodemailer tries to parse an attachments with a embedded file, causing t Regex: /^data:((?:[^;]*;)*(?:[^,]*)),(.*)$/ Path: compile -> getAttachments -> _processDataUrl Regex: /(<img\b[^> [^"'>\s]+)/ Path: _convertDataImages ### PoC https://gist.github.com/francoatmega/890dd5053375333e40c6fdbcc francoatmega/9aab042b0b24968d7b7039818e8b2698 ### Impact ReDoS causes the event loop to stuck a specially
RHSA-2022:4991	XZ Utils is an integrated collection of user-space file compression utilities based on the Lempel-Ziv-Markov chain data compression. The algorithm provides a high compression ratio while keeping the decompression time short.
RHSA-2022:5056	The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar oper
RHSA-2022:5311	The libgcrypt library provides general-purpose implementations of various cryptographic algorithms.
RHSA-2022:5313	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2022:5314	Expat is a C library for parsing XML documents.
RHSA-2022:5317	The libxml2 library is a development toolbox providing the implementation of various XML standards.
RHSA-2022:5696	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Sof
RHSA-2022:5809	The pcre2 package contains a new generation of the Perl Compatible Regular Expression libraries for implementin the same syntax and semantics as Perl.
RHSA-2022:6159	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2022:6180	The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring too
RHSA-2022:6206	The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LS parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemo Linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automo transactional dependency-based service control logic. It can also work as a drop-in replacement for sysvinit.
RHSA-2022:6457	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exce and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing
RHSA-2022:6463	The GNU Privacy Guard (GnuPG or GPG) is a tool for encrypting data and creating digital signatures, compliant w
RHSA-2022:6878	Expat is a C library for parsing XML documents.
RHSA-2022:7006	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Sof
RHSA-2022:7089	KSBA (pronounced Kasbah) is a library to make X.509 certificates as well as the CMS easily accessible by other a blocks of S/MIME and TLS.
RHSA-2022:7105	The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptograph TLS, and DTLS.
RHSA-2022:7106	The zlib packages provide a general-purpose lossless data compression library that is used by many different progr
RHSA-2022:7108	SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and fle administrative hassles of supporting a separate database server.
RHSA-2022:7704	WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform.
RHSA-2022:7715	The libxml2 library is a development toolbox providing the implementation of various XML standards.
RHSA-2022:7720	The e2fsprogs packages provide a number of utilities for creating, checking, modifying, and correcting the ext2, ex
RHSA-2022:7745	FreeType is a free, high-quality, portable font engine that can open and manage font files. FreeType loads, hints, ar
RHSA-2022:7793	The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring too
RHSA-2023:0110	SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and fle administrative hassles of supporting a separate database server.
RHSA-2023:0200	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2023:0208	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Sof
RHSA-2023:1095	The zlib packages provide a general-purpose lossless data compression library that is used by many different progr

RHSA-2023:1140	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:1252	Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of securit
RHSA-2023:1332	Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of securit
RHSA-2023:1335	OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protoco cryptography library.
RHSA-2023:1895	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2023:1908	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Sof
RHSA-2023:2963	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:2963	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:3106	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:3555	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exce and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing
RHSA-2023:4175	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2023:4176	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Sof
RHSA-2023:4864	The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar oper
RHSA-2023:5615	The libssh2 packages provide a library that implements the SSH2 protocol.
RHSA-2023:5731	The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Sof
RHSA-2023:5742	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2023:5998	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exce and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing
RHSA-2023:6885	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exce and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing
RHSA-2023:7034	Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exce and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing
RHSA-2023:7743	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2023:7783	PostgreSQL is an advanced object-relational database management system (DBMS).
RHSA-2024:0266	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2024:0533	The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptograph TLS, and DTLS.
RHSA-2024:0606	OpenSSH is an SSH protocol implementation supported by a number of Linux, UNIX, and similar operating syste both the OpenSSH client and server.
RHSA-2024:0606	OpenSSH is an SSH protocol implementation supported by a number of Linux, UNIX, and similar operating syste both the OpenSSH client and server.
RHSA-2024:0811	The sudo packages contain the sudo utility which allows system
RHSA-2024:0894	MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) an
RHSA-2024:1129	The curl packages provide the libcurl library and the curl utility for downloading files from servers using various p
RHSA-2024:1431	Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to pe
RHSA-2024:1510	Node.js is a software development platform for building fast and scalable
RHSA-2024:1822	The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Sof
RHSA-2024:1879	The gnutls package provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographi and DTLS.
RHSA-2024:2463	The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LS parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemo Linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automo transactional dependency-based service control logic. It can also work as a drop-in replacement for sysvinit.

RHSA-2024:2512	The file command is used to identify a particular file according to the type of data the file contains. It can identify r Executable and Linkable Format (ELF) binary files, system libraries, RPM packages, and different graphics format
RHSA-2024:2679	The libxml2 library is a development toolbox providing the implementation of various XML standards.
RHSA-2024:2780	Node.js is a software development platform for building fast and scalable network applications in the JavaScript pr
RHSA-2024:2987	Python is an interpreted, interactive, object-oriented programming language that supports modules, classes, excepti dynamic typing. The python27 packages provide a stable release of Python 2.7 with a number of additional utilities PostgreSQL.
RHSA-2024:2988	The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc
RHSA-2024:3254	The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc
RHSA-2024:3271	The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS s
RHSA-2024:3346	Git Large File Storage (LFS) replaces large files such as audio samples, videos, datasets, and graphics with text poi contents on a remote server.
RHSA-2024:3546	Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to per
RHSA-2024:3588	The glibc packages provide the standard C libraries (libc), POSIX thread
RHSA-2024:3834	The gdk-pixbuf2 packages provide an image loading library that can be extended
RHSA-2024:3968	The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc
SUSE-SU-2023:4659-1	Security update for curl
SUSE-SU-2023:4891-1	Security update for ncurses
SUSE-SU-2024:0070-1	Security update for tar
SUSE-SU-2024:0136-1	Security update for pam
SUSE-SU-2024:0140-1	Security update for libssh
SUSE-SU-2024:0305-1	Security update for cpio
SUSE-SU-2024:0549-1	Security update for openssl-1_1
SUSE-SU-2024:0555-1	Security update for libxml2
SUSE-SU-2024:0973-1	Security update for tiff
SUSE-SU-2024:0997-1	Security update for krb5
SUSE-SU-2024:1014-1	Security update for avahi
SUSE-SU-2024:1103-1	Security update for qemu
SUSE-SU-2024:1129-1	Security update for expat
SUSE-SU-2024:1133-1	Security update for ncurses
SUSE-SU-2024:1136-1	Security update for c-ares
SUSE-SU-2024:1151-1	Security update for curl
SUSE-SU-2024:1167-1	Security update for nghttp2
SUSE-SU-2024:1172-1	Security update for util-linux
SUSE-SU-2024:1271-1	Security update for gnutls
SUSE-SU-2024:1438-1	Security update for qemu
SUSE-SU-2024:1981-1	Security update for iperf
TEMP-0000000-F7A20F	Kernel: Unpriviledged user can freeze journald