



# CVE-2023-4921

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2023-4921   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | security@google.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2023-09-12 20:15:00 UTC   |
| <b>Updated</b>         | 2023-10-29 02:39:00 UTC   |
| <b>Description</b>     | A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege |

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                      | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |

## References

| Reference  | Source  | Link                             | Tags                |
|--|---------|----------------------------------|---------------------|
| [SECURITY] [DLA 3623-1] linux-5.10 security update       | MISC    | <a href="#">lists.debian.org</a> |                     |
| kernel.dance/8fc134fee27f2263988ae38920bc03da416b03d8    | MISC    | <a href="#">kernel.dance</a>     |                     |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC    | <a href="#">git.kernel.org</a>   |                     |
| CVE Program record                                       | CVE.ORG | <a href="#">www.cve.org</a>      | canonical           |
| NVD vulnerability detail                                 | NVD     | <a href="#">nvd.nist.gov</a>     | canonical, analysis |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[161237](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-13043)

[161334](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2024-12110)

[161372](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2024-12169)

|  |
|--|
| <a href="#">161402</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2024-0897)                     |
| <a href="#">161426</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2024-1249)                     |
| <a href="#">199841</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6444-1)              |
| <a href="#">199842</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6440-1)              |
| <a href="#">199843</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6439-1)              |
| <a href="#">199844</a> Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6445-1) |
| <a href="#">199845</a> Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6442-1)  |
| <a href="#">199846</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6441-1)              |
| <a href="#">199848</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6446-1)              |
| <a href="#">199849</a> Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-6440-2)      |
| <a href="#">199854</a> Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-6441-2)        |
| <a href="#">199855</a> Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6439-2)        |
| <a href="#">199858</a> Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6445-2) |
| <a href="#">199859</a> Ubuntu Security Notification for Linux kernel (StarFive) Vulnerabilities (USN-6444-2)   |
| <a href="#">199861</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6446-2)              |
| <a href="#">199864</a> Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-6440-3)        |
| <a href="#">199868</a> Ubuntu Security Notification for Linux kernel (Oracle) Vulnerabilities (USN-6446-3)     |
| <a href="#">199872</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6441-3)              |
| <a href="#">199881</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6461-1)        |
| <a href="#">199883</a> Ubuntu Security Notification for Linux kernel (NVIDIA) Vulnerabilities (USN-6466-1)     |
| <a href="#">199893</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6479-1)        |
| <a href="#">199912</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6454-1)              |
| <a href="#">199913</a> Ubuntu Security Notification for Linux kernel (StarFive) Vulnerabilities (USN-6454-4)   |
| <a href="#">199916</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6454-2)              |
| <a href="#">199918</a> Ubuntu Security Notification for Linux kernel (ARM laptop) Vulnerabilities (USN-6454-3) |
| <a href="#">200201</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6699-1)              |
| <a href="#">242785</a> Red Hat Update for kpatch-patch (RHSA-2024:0593)  |
| <a href="#">242830</a> Red Hat Update for kernel-rt (RHSA-2024:0563)   |

|   |
|---|
| <a href="#">242831</a> Red Hat Update for kernel (RHSA-2024:0562)                                       |
| <a href="#">242890</a> Red Hat Update for kernel (RHSA-2024:0724)                                       |
| <a href="#">242931</a> Red Hat Update for kpatch-patch (RHSA-2024:0851)                                 |
| <a href="#">242938</a> Red Hat Update for kpatch-patch (RHSA-2024:0876)                                 |
| <a href="#">242939</a> Red Hat Update for kernel (RHSA-2024:0897)                                       |
| <a href="#">242983</a> Red Hat Update for kernel-rt (RHSA-2024:0881)                                    |
| <a href="#">243051</a> Red Hat Update for kernel (RHSA-2024:1249)                                       |
| <a href="#">243055</a> Red Hat Update for kernel (RHSA-2024:1268)                                       |
| <a href="#">243057</a> Red Hat Update for kpatch-patch (RHSA-2024:1278)                                 |
| <a href="#">243058</a> Red Hat Update for kernel-rt (RHSA-2024:1269)                                    |
| <a href="#">243068</a> Red Hat Update for kpatch-patch (RHSA-2024:1323)                                 |
| <a href="#">243071</a> Red Hat Update for kernel-rt (RHSA-2024:1332)                                    |
| <a href="#">243078</a> Red Hat Update for kpatch-patch (RHSA-2024:1368)                                 |
| <a href="#">243087</a> Red Hat Update for kernel (RHSA-2024:1404)                                       |
| <a href="#">257311</a> CentOS Security Update for kernel (CESA-2024:1249)                               |
| <a href="#">356357</a> Amazon Linux Security Advisory for kernel : ALAS-2023-1838                       |
| <a href="#">356371</a> Amazon Linux Security Advisory for kernel : ALAS2023-2023-356                    |
| <a href="#">356409</a> Amazon Linux Security Advisory for kernel : ALAS2-2023-2264                      |
| <a href="#">356567</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-027            |
| <a href="#">356571</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-155    |
| <a href="#">356572</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-040            |
| <a href="#">356577</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-150    |
| <a href="#">356584</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-152    |
| <a href="#">356588</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-154    |
| <a href="#">356595</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-153    |
| <a href="#">356599</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-151    |
| <a href="#">356606</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-053             |
| <a href="#">356611</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-149    |
| <a href="#">356919</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-026 |

|   |
|---|
| <a href="#">356923</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-024               |
| <a href="#">356924</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-025               |
| <a href="#">379043</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)                    |
| <a href="#">379435</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2024:0012)                    |
| <a href="#">390294</a> Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2024-0002) |
| <a href="#">6000265</a> Debian Security Update for linux-5.10 (DLA 3623-1)  |
| <a href="#">6000429</a> Debian Security Update for linux (DLA 3710-1)   |
| <a href="#">6140163</a> AWS Bottlerocket Security Update for kernel (GHSA-prvh-4x5m-5x39)                             |
| <a href="#">673406</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3182)                                      |
| <a href="#">673563</a> EulerOS Security Update for kernel (EulerOS-SA-2024-1144)                                      |
| <a href="#">673595</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3247)                                      |
| <a href="#">673644</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3336)                                      |
| <a href="#">673692</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3275)                                      |
| <a href="#">673848</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3217)                                      |
| <a href="#">673995</a> EulerOS Security Update for kernel (EulerOS-SA-2024-1275)                                      |
| <a href="#">674042</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3304)                                      |
| <a href="#">755059</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4035-1)               |
| <a href="#">755060</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4031-1)               |
| <a href="#">755061</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4030-1)               |
| <a href="#">755063</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4032-1)               |
| <a href="#">755082</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4058-1)               |
| <a href="#">755083</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4057-1)               |
| <a href="#">755085</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4072-1)               |
| <a href="#">755086</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4071-1)               |
| <a href="#">755096</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4093-1)               |
| <a href="#">755107</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4095-1)               |
| <a href="#">755229</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4072-2)               |
| <a href="#">755565</a> SUSE Security Update for the linux kernel (SUSE-SU-2023:4347-1)                                |

|  |
|--|
| 755747 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0469-1)                                  |
| 755751 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0474-1)                                  |
| 755752 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0478-1)                                  |
| 755754 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0516-1)                                  |
| 755755 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0515-1)                                  |
| 755756 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0514-1)                                  |
| 755837 SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 5 for SLE 15 SP5) (SUSE-SU-2024:0624-1) |
| 755838 SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 3 for SLE 15 SP5) (SUSE-SU-2024:0622-1) |
| 755860 SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2024:0655-1) |
| 755865 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 33 for SLE 15 SP2) (SUSE-SU-2024:0666-1)   |
| 755868 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 5 for SLE 15 SP5) (SUSE-SU-2024:0685-1)    |
| 755869 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 8 for SLE 15 SP4) (SUSE-SU-2024:0698-1)    |
| 755871 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 1 for SLE 15 SP5) (SUSE-SU-2024:0727-1)    |
| 907387 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (28779-1)                                      |
| 941584 AlmaLinux Security Update for kernel (ALSA-2024:0897)   |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**