



# CVE-2023-4207

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

## Summary

<b>CVE</b>	CVE-2023-4207
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-06 14:15:00 UTC
<b>Updated</b>	2024-02-05 19:55:00 UTC
<b>Description</b>	A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local privilege e

## 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>	12.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="#">kernel.dance/76e42ae831991c828cfa8c37736ebfb831ad5ec</a>	MISC	<a href="#">kernel.dance</a>	
<a href="#">kernel/git/torvalds/linux.git - Linux kernel source tree</a>	MISC	<a href="#">git.kernel.org</a>	
<a href="#">lists.debian.org/debian-lts-announce/2024/01/msg00004.html</a>		<a href="#">lists.debian.org</a>	Mailing List, Third Party Advisory, VDB Entry
<a href="#">Debian -- Security Information -- DSA-5492-1 linux</a>	MISC	<a href="#">www.debian.org</a>	
<a href="#">CVE Program record</a>	CVE.ORG	<a href="#">www.cve.org</a>	canonical
<a href="#">NVD vulnerability detail</a>	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[161066](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-6583)

[161147](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-7077)

<a href="#">161194</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2023-7423)
<a href="#">161211</a> Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-13019)
<a href="#">242399</a> Red Hat Update for kernel security (RHSA-2023:6583)
<a href="#">242434</a> Red Hat Update for kernel-rt security (RHSA-2023:6901)
<a href="#">242451</a> Red Hat Update for kernel security (RHSA-2023:7077)
<a href="#">242482</a> Red Hat Update for kernel-rt (RHSA-2023:7379)
<a href="#">242497</a> Red Hat Update for kpatch-patch (RHSA-2023:7418)
<a href="#">242498</a> Red Hat Update for kernel-rt (RHSA-2023:7424)
<a href="#">242501</a> Red Hat Update for kernel (RHSA-2023:7423)
<a href="#">242502</a> Red Hat Update for kpatch-patch (RHSA-2023:7419)
<a href="#">242518</a> Red Hat Update for kpatch-patch (RHSA-2023:7558)
<a href="#">242521</a> Red Hat Update for kernel security (RHSA-2023:7539)
<a href="#">242612</a> Red Hat Update for kernel security (RHSA-2023:7370)
<a href="#">257270</a> Centos Security Update for kernel
<a href="#">257295</a> CentOS Security Update for kernel (CESA-2023:7423)
<a href="#">356357</a> Amazon Linux Security Advisory for kernel : ALAS-2023-1838
<a href="#">356409</a> Amazon Linux Security Advisory for kernel : ALAS2-2023-2264
<a href="#">356571</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-155
<a href="#">356578</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-054
<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="#">390293</a> Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2023-0025)
<a href="#">6000220</a> Debian Security Update for linux (DSA 5492-1)
<a href="#">6000429</a> Debian Security Update for linux (DLA 3710-1)
<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)

[673848](#) EulerOS Security Update for kernel (EulerOS-SA-2023-3217)

[907297](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (28678-1)

[941453](#) AlmaLinux Security Update for kernel (ALSA-2023:7077)

© [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](#)