



CVE-2023-35788

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

Summary

CVE	CVE-2023-35788
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-16 21:15:00 UTC
Updated	2023-11-02 01:36:00 UTC
Description	An issue was discovered in fl_set_geneve_opt in net/sched/cls_flower.c in the Linux kernel before 6.3.7. It allows an out-of-

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	22.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	12.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All

Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference	Source	Link	Tags
cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3.7	MISC	cdn.kernel.org	
Kernel Live Patch Security Notice LSN-0097-1 ≈ Packet Storm	MISC	packetstormsecurity.com	
[SECURITY] [DLA 3508-1] linux security update	MLIST	lists.debian.org	
403 Forbidden	CONFIRM	security.netapp.com	
Debian -- Security Information -- DSA-5480-1 linux	DEBIAN	www.debian.org	
oss-security - Linux kernel: off-by-one in fl_set_geneve_opt	MISC	www.openwall.com	
oss-security - Re: Linux kernel: off-by-one in fl_set_geneve_opt	MLIST	www.openwall.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
Debian -- Security Information -- DSA-5448-1 linux	DEBIAN	www.debian.org	
[SECURITY] [DLA 3623-1] linux-5.10 security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160837 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-4377)
160934 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-5244)
199441 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6194-1)
199442 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6193-1)
199443 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6192-1)
199452 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6206-1)
199453 Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-6205-1)
199455 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6212-1)
199463 Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-6223-1)
199466 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6220-1)
199470 Ubuntu Security Notification for Linux kernel (Xilinx ZynqMP) Vulnerability (USN-6234-1)
199521 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6235-1)

199614 Ubuntu Security Notification for Linux kernel (IoT) Vulnerabilities (USN-6256-1)
241878 Red Hat Update for kernel security (RHSA-2023:4377)
241880 Red Hat Update for kpatch-patch (RHSA-2023:4380)
241886 Red Hat Update for kernel-rt (RHSA-2023:4378)
241926 Red Hat Update for kernel (RHSA-2023:4515)
241929 Red Hat Update for kpatch-patch (RHSA-2023:4516)
241957 Red Hat Update for kernel (RHSA-2023:4697)
241960 Red Hat Update for kpatch-patch (RHSA-2023:4698)
242062 Red Hat Update for kpatch-patch (RHSA-2023:5221)
242070 Red Hat Update for kernel security (RHSA-2023:5244)
242075 Red Hat Update for kernel-rt (RHSA-2023:5255)
242142 Red Hat Update for kpatch-patch (RHSA-2023:5575)
242154 Red Hat Update for kernel (RHSA-2023:5604)
242157 Red Hat Update for kernel-rt (RHSA-2023:5603)
257254 CentOS Security Update for kernel
355464 Amazon Linux Security Advisory for kernel : ALAS2023-2023-228
355531 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-034
355532 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-021
355536 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-047
355838 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-138
355845 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-141
355850 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-139
355854 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-137
355858 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-140
356518 Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-016
356529 Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-017
356536 Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-019
356543 Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-018

378701 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0030)
378710 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
379043 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)
379090 IBM QRadar SIEM Multiple Security Vulnerabilities (7070736)
6000136 Debian Security Update for linux (DLA 3508-1)
6000207 Debian Security Update for linux (DSA 5448-1)
6000212 Debian Security Update for linux (DSA 5480-1)
6000265 Debian Security Update for linux-5.10 (DLA 3623-1)
6140162 AWS Bottlerocket Security Update for kernel (GHSA-fj24-hr87-wmhv)
673261 EulerOS Security Update for kernel (EulerOS-SA-2023-2614)
673272 EulerOS Security Update for kernel (EulerOS-SA-2023-2584)
673354 EulerOS Security Update for kernel (EulerOS-SA-2023-2843)
673372 EulerOS Security Update for kernel (EulerOS-SA-2023-2787)
673496 EulerOS Security Update for kernel (EulerOS-SA-2023-2860)
673498 EulerOS Security Update for kernel (EulerOS-SA-2023-3132)
673604 EulerOS Security Update for kernel (EulerOS-SA-2023-2811)
754170 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2834-1)
754183 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2859-1)
907041 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27197-1)
907048 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27196-1)
941213 AlmaLinux Security Update for kernel (ALSA-2023:4377)
941214 AlmaLinux Security Update for kernel-rt (ALSA-2023:4378)
941276 AlmaLinux Security Update for kernel (ALSA-2023:5244)
960961 Rocky Linux Security Update for kernel-rt (RLSA-2023:4378)
961022 Rocky Linux Security Update for kernel (RLSA-2023:5244)

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](#)