CVE-2023-35823

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-35823
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-18 22:15:00 UTC
Updated	2023-11-07 04:15:00 UTC
Description	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in saa7134_finidev in drivers/media/pc

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
[PATCH] media: saa7134: fix use after free bug in saa7134_finidev due to race condition	MISC	lore.kernel.org	
[SECURITY] [DLA 3508-1] linux security update	MLIST	lists.debian.org	
[GIT PULL FOR v6.4] Various fixes/enhancements - Hans Verkuil	MISC	lore.kernel.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
[GIT PULL FOR v6.4] Various fixes/enhancements - Hans Verkuil		lore.kernel.org	
cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3.2	MISC	cdn.kernel.org	
June 2023 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] [DLA 3623-1] linux-5.10 security update	MLIST	lists.debian.org	
[PATCH] media: saa7134: fix use after free bug in saa7134_finidev due to race condition		lore.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 161147 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-7077)
- 199652 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6283-1)
- 199670 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6300-1)
- 199784 Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6397-1)
- 242434 Red Hat Update for kernel-rt security (RHSA-2023:6901)
- 242451 Red Hat Update for kernel security (RHSA-2023:7077)
- 242789 Red Hat Update for kernel (RHSA-2024:0575)
- 242855 Red Hat Update for kernel (RHSA-2024:0412)
- 378892 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0114)
- 379043 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)
- 379435 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2024:0012)
- 6000136 Debian Security Update for linux (DLA 3508-1)
- 6000265 Debian Security Update for linux-5.10 (DLA 3623-1)
- 673272 EulerOS Security Update for kernel (EulerOS-SA-2023-2584)
- 673354 EulerOS Security Update for kernel (EulerOS-SA-2023-2843)
- 673496 EulerOS Security Update for kernel (EulerOS-SA-2023-2860)
- 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)
- 907071 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27225-1)
- 907221 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27245-1)
- 941453 AlmaLinux Security Update for kernel (ALSA-2023:7077)

CVE.report and Source URL Uptime Status status.cve.report