CVE-2022-1116

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-1116
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-17 17:15:00 UTC
Updated	2022-10-19 17:46:00 UTC
Description	Integer Overflow or Wraparound vulnerability in io_uring of Linux Kernel allows local attacker to cause memory corruption a

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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
????????	MISC	kernel.dance	
Kernel Live Patch Security Notice LSN-0086-1 ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE-2022-1116 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
kernel/git/stable/linux.git - Linux kernel stable tree	MISC	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonica

NVD vulnerability detail NVD nvd.nist.gov canonica

Vendor Comments And Credit

Discovery Credit

LEGACY: Bing-Jhong Billy Jheng <billy@starlabs.sg>

Legacy QID Mappings

198802 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5442-1)

198812 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5442-2)

610451 Google Pixel Android December 2022 Security Patch Missing

752463 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2809-1)

752502 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2875-1)

753144 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 27 for SLE 15 SP2) (SUSE-SU-2022:2237-1)

753153 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 13 for SLE 15 SP3) (SUSE-SU-2022:2239-1)

753156 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2741-1)

753169 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15 SP2) (SUSE-SU-2022:2230-1)

753234 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15 SP2) (SUSE-SU-2022:3088-1)

753243 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP3) (SUSE-SU-2022:2216-1)

753253 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 15 for SLE 15 SP3) (SUSE-SU-2022:2245-1)

753301 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 22 for SLE 15 SP3) (SUSE-SU-2022:2761-1)

753316 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2892-1)

753353 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 17 for SLE 15 SP3) (SUSE-SU-2022:2262-1)

753378 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 23 for SLE 15 SP3) (SUSE-SU-2022:3080-1)

753415 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 20 for SLE 15 SP3) (SUSE-SU-2022:2516-1)

753486 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 19 for SLE 15 SP3) (SUSE-SU-2022:2214-1)

© 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 registred 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.

Free CVE JSON API cve.report/api

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