



CVE-2018-25020

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

Summary

CVE	CVE-2018-25020
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-08 05:15:00 UTC
Updated	2022-04-05 20:55:00 UTC
Description	The BPF subsystem in the Linux kernel before 4.17 mishandles situations with a long jump over an instruction sequence w

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	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	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All

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

References

Reference	Source	Link	Tags
CVE-2018-25020 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
bpf: fix truncated jump targets on heavy expansions · torvalds/linux@050fad7 · GitHub	MISC	github.com	
Kernel Live Patch Security Notice LSN-0083-1 ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

353184 Amazon Linux Security Advisory for kernel : ALAS-2022-1571
353195 Amazon Linux Security Advisory for kernel : ALAS2-2022-1761
610418 Google Pixel Android June 2022 Security Patch Missing
751600 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0068-1)
751602 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0080-1)
751684 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 41 for SLE 12 SP3) (SUSE-SU-2022:0329-1)
751687 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 40 for SLE 12 SP3) (SUSE-SU-2022:0328-1)
751688 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 12 SP3) (SUSE-SU-2022:0325-1)
751689 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 39 for SLE 12 SP3) (SUSE-SU-2022:0327-1)
751695 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0367-1)
751697 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0366-1)
751698 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0362-1)
751701 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0366-1)
751702 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0371-1)
753087 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 22 for SLE 15) (SUSE-SU-2022:0255-1)
753139 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15) (SUSE-SU-2022:0245-1)
753155 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15) (SUSE-SU-2022:0237-1)
753257 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 23 for SLE 15) (SUSE-SU-2022:0243-1)

© [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 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](#)