



CVE-2022-2938

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

Summary

CVE	CVE-2022-2938
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-23 20:15:00 UTC
Updated	2023-01-20 12:50:00 UTC
Description	A flaw was found in the Linux kernel's implementation of Pressure Stall Information. While the feature is disabled by default

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedora	Fedora	35	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
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link	Tags
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	

CVE-2022-2938 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160210 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-7683)
180958 Debian Security Update for linux (CVE-2022-2938)
240815 Red Hat Update for kernel-rt (RHSA-2022:7444)
240817 Red Hat Update for kernel security (RHSA-2022:7683)
243041 Red Hat Update for kernel security (RHSA-2024:1188)
672391 EulerOS Security Update for kernel (EulerOS-SA-2022-2767)
672454 EulerOS Security Update for kernel (EulerOS-SA-2022-2848)
752594 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3293-1)
753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
753167 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3288-1)
903750 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10704) (DEPRECATED)
903793 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10678)
903987 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10704-1)
904129 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10678-1)
905778 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10704-2)
906379 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10678-2)
940732 AlmaLinux Security Update for kernel (ALSA-2022:7683)
940766 AlmaLinux Security Update for kernel-rt (ALSA-2022:7444)
960176 Rocky Linux Security Update for kernel-rt (RLSA-2022:7444)
960184 Rocky Linux Security Update for kernel (RLSA-2022:7683)

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](#)