CVE-2020-25704

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25704
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-02 01:15:00 UTC
Updated	2022-10-25 16:30:00 UTC
Description	A flaw memory leak in the Linux kernel performance monitoring subsystem was found in the way if using PERF_EVENT_IC

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	5.10	rc1	All	All
Operating System	Linux	Linux Kernel	5.10	rc2	All	All
Operating System	Linux	Linux Kernel	5.10	rc1	All	All
Operating System	Linux	Linux Kernel	5.10	rc2	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Starwindsoftware	Command Center	-	All	All	All
Application	Starwindsoftware	Starwind Hyperconverged Appliance	-	All	All	All
Application	Starwindsoftware	Starwind San Nas	v8r12	All	All	All
Application	Starwindsoftware	Starwind Virtual San	v8	build14398	All	All

References

Reference	Source	Link	Ta
[SECURITY] [DLA 2494-1] linux security update	MLIST	lists.debian.org	
CVE-2020-25704 Linux kernel vulnerability in StarWind products	MISC	www.starwindsoftware.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	P
oss-security - [CVE-2020-25704] Linux kernel: perf_event_parse_addr_filter memory leak	MISC	www.openwall.com	M

[SECURITY] [DLA 2483-1] linux-4.19 security update	MLIST	lists.debian.org	
1895961 – (CVE-2020-25704) CVE-2020-25704 kernel: perf_event_parse_addr_filter memory	MISC	bugzilla.redhat.com	ls
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159185 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1578)

159588 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-0063)

239314 Red Hat Update for kernel-rt (RHSA-2021:1739)

239339 Red Hat Update for kernel (RHSA-2021:1578)

239501 Red Hat Update for kernel-rt (RHSA-2021:2719) (Sequoia)

239502 Red Hat Update for kernel (RHSA-2021:2718) (Sequoia)

239989 Red Hat Update for kernel-rt (RHSA-2022:0065)

239997 Red Hat Update for kernel (RHSA-2022:0063)

257142 CentOS Security Update for kernel (CESA-2022:0063)

257144 CentOS Security Update for kernel (CESA-2022:0063)

353100 Amazon Linux Security Advisory for kernel : ALAC2012-2021-024

353101 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025

353102 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026

353133 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-018

376529 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Linux Kernel Vulnerability (K44994972)

377038 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)

6140173 AWS Bottlerocket Security Update for kernel (GHSA-jrx3-x2ph-rj9p)

670185 EulerOS Security Update for kernel (EulerOS-SA-2021-1684)

750376 OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)

750488 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2260-1)

750533 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2112-1)

750568 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2034-1)

750609 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:1906-1)

900040 CBL-Mariner Linux Security Update for kernel 5.4.91

903681 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3642)

905936 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3642-1)

940354 AlmaLinux Security Update for kernel (ALSA-2021:1578)