



# CVE-2020-25704

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-25704
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-02 01:15:00 UTC
<b>Updated</b>	2022-10-25 16:30:00 UTC
<b>Description</b>	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	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.10	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.10	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.10	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.10	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Command Center</a>	-	All	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Hyperconverged Appliance</a>	-	All	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind San Nas</a>	v8r12	All	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build14398	All	All

## References

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

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

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">159185</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1578)
<a href="#">159588</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2022-0063)
<a href="#">239314</a> Red Hat Update for kernel-rt (RHSA-2021:1739)
<a href="#">239339</a> Red Hat Update for kernel (RHSA-2021:1578)
<a href="#">239501</a> Red Hat Update for kernel-rt (RHSA-2021:2719) (Sequoia)
<a href="#">239502</a> Red Hat Update for kernel (RHSA-2021:2718) (Sequoia)
<a href="#">239989</a> Red Hat Update for kernel-rt (RHSA-2022:0065)
<a href="#">239997</a> Red Hat Update for kernel (RHSA-2022:0063)
<a href="#">257142</a> CentOS Security Update for kernel (CESA-2022:0063)
<a href="#">257144</a> CentOS Security Update for kernel (CESA-2022:0063)
<a href="#">353100</a> Amazon Linux Security Advisory for kernel : ALAC2012-2021-024
<a href="#">353101</a> Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025
<a href="#">353102</a> Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026
<a href="#">353133</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-018
<a href="#">376529</a> F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Linux Kernel Vulnerability (K44994972)
<a href="#">377038</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)
<a href="#">6140173</a> AWS Bottlerocket Security Update for kernel (GHSA-jrx3-x2ph-rj9p)
<a href="#">670185</a> EulerOS Security Update for kernel (EulerOS-SA-2021-1684)
<a href="#">750376</a> OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
<a href="#">750488</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2260-1)
<a href="#">750533</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2112-1)
<a href="#">750568</a> 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)

© [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](#)**