



# CVE-2020-25643

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

## Summary

<b>CVE</b>	CVE-2020-25643
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-10-06 14:15:00 UTC
<b>Updated</b>	2023-05-16 10:48:00 UTC
<b>Description</b>	A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read o

## Risk And Classification

### Problem Types: CWE-20

## 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>	10.0	All	All	All
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>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc5	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc6	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc5	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.9.0	rc6	All	All

Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410c Firmware</a>	-	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build12533	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build12658	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build12859	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build13170	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build13586	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build13861	All	All

## References

### Reference

[security-announce] openSUSE-SU-2020:1655-1: important: Security update

[SECURITY] [DLA 2420-2] linux regression update

Debian -- Security Information -- DSA-4774-1 linux

CVE-2020-25643 Linux Kernel vulnerability in StarWind VSAN for vSphere (VSA)

[security-announce] openSUSE-SU-2020:1698-1: important: Security update

CVE-2020-25643 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security

1879981 – (CVE-2020-25643) CVE-2020-25643 kernel: improper input validation in ppp\_cp\_parse\_cr function leads to memory corruption and

[SECURITY] [DLA 2417-1] linux-4.19 security update

kernel/git/torvalds/linux.git - Linux kernel source tree

[SECURITY] [DLA 2420-1] linux security update

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

159185 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1578)
239314 Red Hat Update for kernel-rt (RHSA-2021:1739)
239339 Red Hat Update for kernel (RHSA-2021:1578)
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
377038 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)
750376 OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
750533 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2112-1)
900076 CBL-Mariner Linux Security Update for kernel 5.4.91
902957 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3509)
906038 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3509-1)
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](#)**