



CVE-2020-25645

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

Summary

CVE	CVE-2020-25645
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-13 20:15:00 UTC
Updated	2021-03-26 02:25:00 UTC
Description	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted

Risk And Classification

Problem Types: CWE-319

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.9.0	-	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc1	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc2	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc3	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc4	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc5	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc6	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.9.0	-	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc1	All	All

Operating System	Linux	Linux Kernel	5.9.0	rc2	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc3	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc4	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc5	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc6	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Operating System	Netapp	Hci Compute Node Bios	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Netapp	Solidfire Hci Storage Node	-	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

References

Reference	Source
Debian -- Security Information -- DSA-4774-1 linux	DEBIAN
[security-announce] openSUSE-SU-2020:1698-1: important: Security update	SUSE
[SECURITY] [DLA 2494-1] linux security update	MLIST
Kernel Live Patch Security Notice LSN-0074-1 ≈ Packet Storm	MISC
[SECURITY] [DLA 2417-1] linux-4.19 security update	MLIST
[security-announce] openSUSE-SU-2020:1682-1: important: Security update	SUSE
CVE-2020-25645 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIR
1883988 – (CVE-2020-25645) CVE-2020-25645 kernel: Geneve/IPsec traffic may be unencrypted between two Geneve endpoints	MISC
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

174806 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 39 for SLE 12 SP2) (SUSE-SU-2021:0835-1)
174874 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 38 for SLE 12 SP3) (SUSE-SU-2021:1074-1)
198328 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4912-1)
239151 Red Hat Update for kernel (RHSA-2021:0856)
257070 CentOS Security Update for kernel (CESA-2021:0856)
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

[903192](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3484)

[906177](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3484-1)

© [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](#)