



CVE-2020-10711

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

Summary

CVE	CVE-2020-10711
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-22 15:15:00 UTC
Updated	2023-11-07 03:14:00 UTC
Description	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs

Risk And Classification

Problem Types: CWE-476

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	19.10	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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	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	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Redhat	3scale	2.0	All	All	All
Application	Redhat	3scale	2.0	All	All	All

Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Messaging Realtime Grid	2.0	All	All	All
Operating System	Redhat	Messaging Realtime Grid	2.0	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference

[USN-4412-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu](#)

[USN-4419-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu](#)

[oss-security - CVE-2020-10711 Kernel: NetLabel: null pointer dereference while receiving CIPSO packet with null category](#)

[May 2020 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security](#)

[Debian -- Security Information -- DSA-4699-1 linux](#)

[\[security-announce\] openSUSE-SU-2020:0935-1: important: Security update](#)

[USN-4411-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu](#)

[1825116 – \(CVE-2020-10711\) CVE-2020-10711 Kernel: NetLabel: null pointer dereference while receiving CIPSO packet with null category m](#)

[\[SECURITY\] \[DLA 2242-1\] linux-4.9 security update](#)

[USN-4413-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu](#)

[Debian -- Security Information -- DSA-4698-1 linux](#)

[\[security-announce\] openSUSE-SU-2020:0801-1: important: Security update](#)

[USN-4414-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[352300](#) Amazon Linux Security Advisory for kernel: ALAC2012-2020-020

[352358](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-010

[352359](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-009

[352360](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-008

[352361](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-007

[353140](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-011

[377065](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0113)

[390217](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2021-0001)

[390234](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0001)

[6140132](#) AWS Bottlerocket Security Update for kernel (GHSA-mgxf-pj6m-9494)

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

[900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91

[903697](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3458)

[905988](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3458-1)

© [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](#)