



# CVE-2020-10751

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

## Summary

<b>CVE</b>	CVE-2020-10751
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-05-26 15:15:00 UTC
<b>Updated</b>	2023-02-12 23:39:00 UTC
<b>Description</b>	A flaw was found in the Linux kernels SELinux LSM hook implementation before version 5.7, where it incorrectly assumed t

## Risk And Classification

**Problem Types:** CWE-349

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Kernel</a>	<a href="#">Selinux</a>	All	All	All	All
Application	<a href="#">Kernel</a>	<a href="#">Selinux</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	8.0	All	All	All

## References

Reference	Source	Link	Tags
Re: selinux_netlink_send changes program behavior - Dmitry Vyukov	CONFIRM	<a href="https://lore.kernel.org">lore.kernel.org</a>	Mailin
USN-4412-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
1839634 – (CVE-2020-10751) CVE-2020-10751 kernel: SELinux netlink permission check bypass	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat Customer Portal	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Debian -- Security Information -- DSA-4699-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
USN-4391-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
oss-security - CVE-2020-10751 - Linux kernel: SELinux netlink permission check bypass	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	Mailin

Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
Re: selinux_netlink_send changes program behavior - Dmitry Vyukov	MISC	<a href="https://lore.kernel.org">lore.kernel.org</a>	
USN-4390-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
[security-announce] openSUSE-SU-2020:0935-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
[SECURITY] [DLA 2241-2] linux security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
USN-4389-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
oss-security - Linux kernel SELinux/netlink missing access check	CONFIRM	<a href="https://www.openwall.com">www.openwall.com</a>	Mailin
[SECURITY] [DLA 2242-1] linux-4.9 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
USN-4413-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
1839634 – (CVE-2020-10751) CVE-2020-10751 kernel: SELinux netlink permission check bypass	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue
[SECURITY] [DLA 2241-1] linux security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
Oracle Critical Patch Update Advisory - April 2021	MISC	<a href="https://www.oracle.com">www.oracle.com</a>	
Debian -- Security Information -- DSA-4698-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
Red Hat Customer Portal	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
[security-announce] openSUSE-SU-2020:0801-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canor
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canor

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [159684](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)
- [352300](#) Amazon Linux Security Advisory for kernel: ALAC2012-2020-020
- [353139](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-012
- [377065](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0113)
- [750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
- [940256](#) AlmaLinux Security Update for kernel (ALSA-2020:4431)

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](#)