



# CVE-2020-16166

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

## Summary

<b>CVE</b>	CVE-2020-16166
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-07-30 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:18:00 UTC
<b>Description</b>	The Linux kernel through 5.7.11 allows remote attackers to make observations that help to obtain sensitive information about

## Risk And Classification

### Problem Types: CWE-330

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	All	All	All	All

Application	Netapp	Cloud Volumes Ontap Mediator	-	All	All	All
Application	Netapp	Cloud Volumes Ontap Mediator	-	All	All	All
Application	Netapp	E-series Santricity Os Controller	All	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Application	Netapp	Hci Bootstrap Os	-	All	All	All
Application	Netapp	Hci Bootstrap Os	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Netapp	Storagegrid	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Oracle	Sd-wan Edge	8.2	All	All	All

## References

Reference	Source	Link	Tag
[SECURITY] [DLA 2420-2] linux regression update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Me
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	Pa
USN-4526-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Th
CVE-2020-16166 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	Th
[SECURITY] [DLA 2385-1] linux-4.19 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Me
arxiv.org/pdf/2012.07432.pdf	MISC	<a href="https://arxiv.org">arxiv.org</a>	Te
USN-4525-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Th
[SECURITY] Fedora 32 Update: kernel-5.7.14-200.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Th
[SECURITY] Fedora 31 Update: kernel-5.7.15-100.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Th
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	Pa
[security-announce] openSUSE-SU-2020:1236-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Me
[SECURITY] Fedora 31 Update: kernel-5.7.15-100.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Th

[SECURITY] Fedora 31 Update: kernel-5.7.15-100.fc31 - package-announce - Fedora Mailing-Lists			<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[security-announce] openSUSE-SU-2020:1153-1: important: Security update	SUSE		<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Ma
[SECURITY] [DLA 2420-1] linux security update	MLIST		<a href="https://lists.debian.org">lists.debian.org</a>	Ma
Oracle Critical Patch Update Advisory - April 2021	MISC		<a href="https://www.oracle.com">www.oracle.com</a>	
[SECURITY] Fedora 32 Update: kernel-5.7.14-200.fc32 - package-announce - Fedora Mailing-Lists			<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
random32: update the net random state on interrupt and activity · torvalds/linux@f227e3e · GitHub	MISC		<a href="https://github.com">github.com</a>	Pa
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

- [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
- [353137](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-014
- [377038](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)
- [390237](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2020-0054)
- [750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
- [900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [903475](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (1922)
- [906133](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (1922-1)

© [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](https://status.cve.report)