



# CVE-2019-7222

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

## Summary

<b>CVE</b>	CVE-2019-7222
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-03-21 16:01:00 UTC
<b>Updated</b>	2023-11-07 03:13:00 UTC
<b>Description</b>	The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak.

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## 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>	12.04	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>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	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>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	28	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	28	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

Application	Netapp	Active Iq Performance Analytics Services	-	All	All	All
Application	Netapp	Active Iq Performance Analytics Services	-	All	All	All
Application	Netapp	Element Software Management Node	-	All	All	All
Application	Netapp	Element Software Management Node	-	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time	7	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time	8	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv	7	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv Tus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time Tus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

## References

Reference	Source	Link
1759 - project-zero - Project Zero - Monorail	CONFIRM	<a href="https://bugs.chromium.org">bugs.chromium.org</a>
[SECURITY] Fedora 28 Update: kernel-4.20.8-100.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	<a href="https://git.kernel.org">git.kernel.org</a>

[security-announce] openSUSE-SU-2019:0203-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
oss-security - Linux kernel: three KVM bugs (CVE-2019-6974, CVE-2019-7221, CVE-2019-7222)	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
USN-3932-2: Linux kernel (Xenial HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
[SECURITY] [DLA 1731-2] linux regression update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 28 Update: kernel-4.20.8-100.fc28 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
USN-3930-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
USN-3930-2: Linux kernel (HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[SECURITY] [DLA 1771-1] linux-4.9 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
USN-3932-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
USN-3933-2: Linux kernel (Trusty HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
History for arch/x86/kvm - torvalds/linux · GitHub	MISC	<a href="https://github.com">github.com</a>
USN-3931-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[SECURITY] [DLA 1731-1] linux security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
March 27th 2019 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
USN-3931-2: Linux kernel (HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
USN-3933-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
KVM kvm_inject_page_fault Uninitialized Memory Leak ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>
Linux Kernel CVE-2019-7222 Local Information Disclosure Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
[SECURITY] Fedora 29 Update: kernel-4.20.8-200.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
[SECURITY] Fedora 29 Update: kernel-4.20.8-200.fc29 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web](https://www.mitre.org/cve)

[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)