



CVE-2019-14821

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-14821
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-19 18:15:00 UTC
Updated	2023-02-12 23:34:00 UTC
Description	An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hyper

Risk And Classification

Problem Types: CWE-787

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	19.04	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	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.4	rc1	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	Aff A700s	-	All	All	All
Operating System	Netapp	Aff A700s Firmware	-	All	All	All
Application	Netapp	Data Availability Services	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All

Operating System	Netapp	H300e Firmware	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H610s	-	All	All	All
Operating System	Netapp	H610s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Oracle	Sd-wan Edge	7.3	All	All	All
Application	Oracle	Sd-wan Edge	8.0	All	All	All
Application	Oracle	Sd-wan Edge	8.1	All	All	All
Application	Oracle	Sd-wan Edge	8.2	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	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	5.0	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 Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Eus	7.7	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 Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	MISC	access.redhat.co
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-311-01)	BUGTRAQ	seclists.org
Red Hat Customer Portal	REDHAT	access.redhat.co
Red Hat Customer Portal	REDHAT	access.redhat.co
September 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.c
[SECURITY] [DLA 1930-1] linux security update	MLIST	lists.debian.org
Red Hat Customer Portal	REDHAT	access.redhat.co
Red Hat Customer Portal	REDHAT	access.redhat.co
[security-announce] openSUSE-SU-2019:2307-1: important: Security update	SUSE	lists.opensuse.or
[SECURITY] Fedora 29 Update: kernel-headers-5.2.17-100.fc29 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraprojec
USN-4162-2: Linux kernel (Azure) vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-4162-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] Fedora 30 Update: kernel-5.2.16-200.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraprojec
Slackware Security Advisory - Slackware 14.2 kernel Updates ≈ Packet Storm	MISC	packetstormsecu
[SECURITY] Fedora 29 Update: kernel-headers-5.2.17-100.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraprojec
USN-4163-2: Linux kernel (Xenial HWE) vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-4157-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
Red Hat Customer Portal	REDHAT	access.redhat.co
USN-4163-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
[security-announce] openSUSE-SU-2019:2308-1: important: Security update	SUSE	lists.opensuse.or
oss-security - CVE-2019-14821 Kernel: KVM: OOB memory access via mmio ring buffer	MLIST	www.openwall.cc
Red Hat Customer Portal	REDHAT	access.redhat.co
USN-4157-2: Linux kernel (HWE) vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com

[SECURITY] [DLA 1940-1] linux-4.9 security update	MLIST	lists.debian.org
Red Hat Customer Portal	REDHAT	access.redhat.co
Debian -- Security Information -- DSA-4531-1 linux	DEBIAN	www.debian.org
Kernel Live Patch Security Notice LSN-0058-1 ≈ Packet Storm	MISC	packetstormsecu
[SECURITY] Fedora 30 Update: kernel-5.2.16-200.fc30 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraprojec
1746708 – (CVE-2019-14821) CVE-2019-14821 Kernel: KVM: OOB memory access via mmio ring buffer	CONFIRM	bugzilla.redhat.co
Bugtraq: [SECURITY] [DSA 4531-1] linux security update	BUGTRAQ	seclists.org
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.co
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle.com
Red Hat Customer Portal	REDHAT	access.redhat.co
1746708 – (CVE-2019-14821) CVE-2019-14821 Kernel: KVM: OOB memory access via mmio ring buffer	MISC	bugzilla.redhat.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376882](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2019:0121)

© [CVE.report](https://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 site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report