CVE-2019-6974

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-6974
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-15 15:29:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference counting because

Risk And Classification

Problem Types: CWE-362 | CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
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	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
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	18.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All

Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All

References

Reference	Source	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
Red Hat Customer Portal	REDHAT	access.redhat.c
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.156	MISC	cdn.kernel.org
support.f5.com/csp/article/K11186236	CONFIRM	support.f5.com
USN-3932-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] [DLA 1731-2] linux regression update	MLIST	lists.debian.org
USN-3930-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3930-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] [DLA 1771-1] linux-4.9 security update	MLIST	lists.debian.org
Red Hat Customer Portal	REDHAT	access.redhat.c
1765 - project-zero - Project Zero - Monorail	MISC	bugs.chromium.
USN-3932-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3933-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.14.99	MISC	cdn.kernel.org
USN-3931-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] [DLA 1731-1] linux security update	MLIST	lists.debian.org

USN-3931-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3933-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Linux - 'kvm_ioctl_create_device()' NULL Pointer Dereference - Linux dos Exploit	EXPLOIT-DB	www.exploit-db.
Linux Kernel CVE-2019-6974 Security Bypass Vulnerability	BID	www.securityfoc
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.20.8	MISC	cdn.kernel.org
Red Hat Customer Portal	REDHAT	access.redhat.c
myF5		support.f5.com
Red Hat Customer Portal	REDHAT	access.redhat.c
support.f5.com/csp/article/K11186236	CONFIRM	support.f5.com
kvm: fix kvm_ioctl_create_device() reference counting (CVE-2019-6974) · torvalds/linux@cfa3938 · GitHub	MISC	github.com
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.21	MISC	cdn.kernel.org
Red Hat Customer Portal	REDHAT	access.redhat.c
Red Hat Customer Portal	REDHAT	access.redhat.c
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

670269 EulerOS Security Update for kernel (EulerOS-SA-2021-1808)

670634 EulerOS Security Update for kernel (EulerOS-SA-2021-2392)

© 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 registred 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