CVE-2019-14835

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-14835
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-17 16:15:00 UTC
Updated	2023-12-15 15:29:00 UTC
Description	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translate

Risk And Classification

Problem Types: CWE-120

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	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	19.04	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	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
Application	Huawei	Imanager Neteco	v600r009c00	All	All	All
Application	Huawei	Imanager Neteco	v600r009c10spc200	All	All	All
Application	Huawei	Imanager Neteco 6000	v600r008c10spc300	All	All	All
Application	Huawei	Imanager Neteco 6000	v600r008c20	All	All	All

Application	Huawei	Manageone	6.5.0	All	All	All
Application	Huawei	Manageone	6.5.0.spc100.b210	All	All	All
Application	Huawei	Manageone	6.5.1rc1.b060	All	All	All
Application	Huawei	Manageone	6.5.1rc1.b080	All	All	All
Application	Huawei	Manageone	6.5.rc2.b050	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.3	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	Aff A700s	All	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	All
Operating System	Netapp	H300e Firmware	-	All	All	All
Hardware	Netapp	H300s	All	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	All	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	All	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500e	All	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	All	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H610s	All	All	All	All
Operating System	Netapp	H610s Firmware	-	All	All	All
Hardware	Netapp	H700e	All	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	All	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Service Processor	-	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
Operating System	Opensuse	Leap	15.0	All	All	All

Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	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	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	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	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	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	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	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	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	7.7	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	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference	Source
Red Hat Customer Portal	REDHA
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-311-01)	BUGTF
oss-security - Re: CVE-2019-14835: QEMU-KVM Guest to Host Kernel Escape Vulnerability: vhost/vhost_net kernel buffer overflow	MLIST
USN-4135-2: Linux kernel vulnerabilities | Ubuntu security notices	UBUNT
USN-4135-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	UBUNT
VHOST-NET GUEST TO HOST ESCAPE - Kernel vulnerability - CVE-2019-14835 - Red Hat Customer Portal	MISC
Red Hat Customer Portal	REDHA
1750727 – (CVE-2019-14835) CVE-2019-14835 kernel: vhost-net: guest to host kernel escape during migration	CONFI
[SECURITY] [DLA 1930-1] linux security update	MLIST
Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA
[SECURITY] Fedora 30 Update: kernel-5.2.15-200.fc30 - package-announce - Fedora Mailing-Lists	FEDOF
Red Hat Customer Portal	REDHA
[SECURITY] Fedora 29 Update: kernel-headers-5.2.17-100.fc29 - package-announce - Fedora Mailing-Lists	MISC
oss-security - Re: CVE-2019-14835: QEMU-KVM Guest to Host Kernel Escape Vulnerability: vhost/vhost_net kernel buffer overflow	MLIST
[security-announce] openSUSE-SU-2019:2181-1: important: Security update	SUSE
Red Hat Customer Portal	REDHA
oss-security - CVE-2019-14835: QEMU-KVM Guest to Host Kernel Escape Vulnerability: vhost/vhost_net kernel buffer overflow	MISC
Red Hat Customer Portal	REDHA
Slackware Security Advisory - Slackware 14.2 kernel Updates ≈ Packet Storm	MISC
oss-security - Re: CVE-2019-14835: QEMU-KVM Guest to Host Kernel Escape Vulnerability: vhost/vhost_net kernel buffer overflow	MLIST
Kernel Live Patch Security Notice LSN-0056-1 ≈ Packet Storm	MISC
[SECURITY] Fedora 29 Update: kernel-headers-5.2.17-100.fc29 - package-announce - Fedora Mailing-Lists	FEDOF
[security-announce] openSUSE-SU-2019:2173-1: important: Security update	SUSE
1750727 – (CVE-2019-14835) CVE-2019-14835 kernel: vhost-net: guest to host kernel escape during migration	MISC
oss-security - Re: CVE-2019-14835: QEMU-KVM Guest to Host Kernel Escape Vulnerability: vhost/vhost_net kernel buffer overflow	MLIST
[SECURITY] Fedora 30 Update: kernel-5.2.15-200.fc30 - package-announce - Fedora Mailing-Lists	MISC
Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA

Red Hat Customer Portal	REDHA
Red Hat Customer Portal	MISC
Red Hat Customer Portal	REDHA
[SECURITY] [DLA 1940-1] linux-4.9 security update	MLIST
Debian -- Security Information -- DSA-4531-1 linux	DEBIAN
Kernel Live Patch Security Notice LSN-0058-1 ≈ Packet Storm	MISC
Security Advisory - Buffer Overflow Vulnerability in QEMU-KVM	CONFI
Red Hat Customer Portal	REDHA
Bugtraq: [SECURITY] [DSA 4531-1] linux security update	BUGTF
Red Hat Customer Portal	REDHA
October 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	CONFI
Red Hat Customer Portal	REDHA
CVE Program record	CVE.O
NVD vulnerability detail	NVD

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)