CVE-2018-1068

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-1068
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-16 16:29:00 UTC
Updated	2023-06-21 15:56:00 UTC
Description	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged us

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	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	17.10	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	17.10	All	All	All
Operating System	Debian	Debian Linux	7.0	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	Debian	Debian Linux	7.0	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	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	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 Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	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	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference	Sour
Debian -- Security Information -- DSA-4188-1 linux	DEB
USN-3674-1: Linux kernel vulnerabilities | Ubuntu security notices	UBU
USN-3674-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	UBU
Red Hat Customer Portal	RED
'BUG: unable to handle kernel paging request in compat_copy_entries' - MARC	MLIS
kernel/git/torvalds/linux.git - Linux kernel source tree	CON
Linux Kernel CVE-2018-1068 Local Privilege Escalation Vulnerability	BID
'[PATCH net] netfilter: check for out-of-bounds while copying compat entries' - MARC	MLIS
Red Hat Customer Portal	RED
Debian -- Security Information -- DSA-4187-1 linux	DEB
[SECURITY] [DLA 1369-1] linux security update	MLIS
USN-3654-1: Linux kernel vulnerabilities | Ubuntu security notices	UBU
netfilter: ebtables: CONFIG_COMPAT: don't trust userland offsets · torvalds/linux@b718121 · GitHub	CON
Red Hat Customer Portal	RED
USN-3654-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	UBU
Red Hat Customer Portal	RED
USN-3656-1: Linux kernel (Raspberry Pi 2, Snapdragon) vulnerabilities | Ubuntu security notices	UBU

USN-3677-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices	UBU
Red Hat Customer Portal	RED
Red Hat Customer Portal	RED
USN-3677-1: Linux kernel vulnerabilities | Ubuntu security notices	UBU
1552048 – (CVE-2018-1068) CVE-2018-1068 kernel: Out-of-bounds write via userland offsets in ebt_entry struct in netfilter/ebtables.c	CON
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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