CVE-2016-4997

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

Summary

CVE	CVE-2016-4997
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-03 21:59:00 UTC
Updated	2023-09-12 14:55:00 UTC
Description	The compat IPT_SO_SET_REPLACE and IP6T_SO_SET_REPLACE setsockopt implementations in the netfilter subsyster

Risk And Classification

Problem Types: CWE-264

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	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	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	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Live Patching	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Live Patching	12.0	All	All	All

Operating System	Novell	Suse Linux Enterprise Module For Public Cloud	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Module For Public Cloud	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	sp1	All	All
Operating System	Oracle	Linux	7	All	All	All
Operating System	Oracle	Linux	7	All	All	All

References

Reference	Sc
USN-3018-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	UE
Red Hat Customer Portal	MI
USN-3016-3: Linux kernel (Qualcomm Snapdragon) vulnerabilities | Ubuntu	UE
Red Hat Customer Portal	RE
[security-announce] SUSE-SU-2016:2177-1: important: Security update for	SU
oss-security - CVE request - Linux kernel through 4.6.2 allows escalade privileges via IP6T_SO_SET_REPLACE compat setsockopt call	ML
TriforceLinuxSyscallFuzzer/crash_reports/report_compatIpt at master · nccgroup/TriforceLinuxSyscallFuzzer · GitHub	MI
USN-3016-1: Linux kernel vulnerabilities | Ubuntu	UE
oss-security - Linux CVE-2016-4997 (local privilege escalation) and CVE-2016-4998 (out of bounds memory access)	ML
[security-announce] SUSE-SU-2016:1937-1: important: Security update for	SU
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.6.3	CO
HPE Support document - HPE Support Center	CO

USN-3017-3: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	UB
Linux Kernel Multiple Local Memory Corruption Vulnerabilities	BI
Oracle Linux Bulletin - July 2016	CC
Oracle Linux Bulletin - October 2016	CC
Red Hat Customer Portal	MI
[security-announce] SUSE-SU-2016:1985-1: important: Security update for	SU
[security-announce] SUSE-SU-2016:1709-1: important: Security update for	SU
USN-3017-1: Linux kernel vulnerabilities | Ubuntu	UB
USN-3017-2: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	UB
USN-3016-4: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu	UB
kernel/git/torvalds/linux.git - Linux kernel source tree	CC
[security-announce] SUSE-SU-2016:2174-1: important: Security update for	SU
netfilter: x_tables: check for bogus target offset · torvalds/linux@ce683e5 · GitHub	CC
Red Hat Customer Portal	RE
USN-3019-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	UB
[security-announce] SUSE-SU-2016:2179-1: important: Security update for	SU
Debian -- Security Information -- DSA-3607-1 linux	DE
[security-announce] SUSE-SU-2016:2018-1: important: Security update for	SU
Oracle VM Server for x86 Bulletin - October 2016	CC
Red Hat Customer Portal	RE
CVE-2016-4997 - Red Hat Customer Portal	MI
USN-3020-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	UB
USN-3016-2: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	UB
[security-announce] SUSE-SU-2016:2180-1: important: Security update for	SU
Red Hat Customer Portal	MI
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Privilege Escalation	EX
[security-announce] SUSE-SU-2016:2105-1: important: Security update for	SU
Linux Kernel 4.6.3 (x86) - 'Netfilter' Local Privilege Escalation (Metasploit) - Linux_x86 local Exploit	EX
[security-announce] openSUSE-SU-2016:2184-1: important: Security update	SU
[security-announce] SUSE-SU-2016:1710-1: important: Security update for	SU
[security-announce] SUSE-SU-2016:2181-1: important: Security update for	SU
Linux Kernel setsockopt() Bugs Let Local Users Deny Service and Gain Elevated Privileges - SecurityTracker	SE
1349722 – (CVE-2016-4997) CVE-2016-4997 kernel: compat IPT_SO_SET_REPLACE setsockopt	CC
[security-announce] SUSE-SU-2016:2178-1: important: Security update for	SU
USN-3018-1: Linux kernel vulnerabilities | Ubuntu	UB
CVE Program record	CV

NVD vulnerability detail NV

No vendor comments have been submitted for this CVE.

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