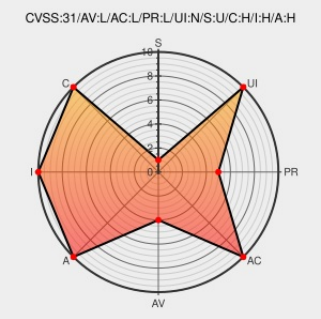
CVE-2016-3135

Published on: 04/27/2016 12:00:00 AM UTC

Last Modified on: 01/17/2023 09:40:00 PM UTC

CVE-2016-3135

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Integer overflow in the xt_alloc_table_info function in net/netfilter/x_tables.c in the Linux kernel through 4.5.2 on 32-bit platforms allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.

CVE-2016-3135 has been assigned by ot security@microfocus.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Linux Kernel Local Memory Corruption and Integer Overflow Vulnerabilities	Third Party Advisory VDB Entry cve.report (archive)	BID 84305

	text/html	
USN-3055-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3055-1
USN-2930-3: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2930-3
USN-3054-1: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3054-1
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=d157bd761585605b7882935ffb86286919f62ea1
USN-2930-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2930-1
netfilter: x_tables: check for size overflow · torvalds/linux@d157bd7 · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/d157bd761585605b7882935ffb86286919f62ea1
USN-2930-2: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2930-2
USN-3057-1: Linux kernel (Qualcomm Snapdragon) vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3057-1
USN-3056-1: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3056-1
1317386 – (CVE-2016-3135) CVE-2016-3135 kernel: netfilter: size overflow in x_tables	Issue Tracking bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1317386
758 - project-zero - Project Zero - Monorail	Third Party Advisory code.google.com text/html	MISC code.google.com/p/google-security-research/issues/detail?id=758

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

- cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→