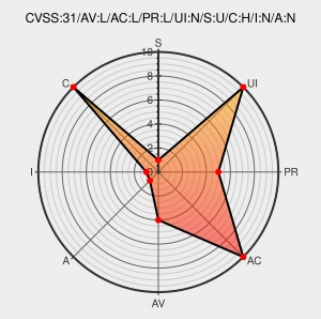
CVE-2016-2383

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

Last Modified on: 01/31/2022 06:55:00 PM UTC

CVE-2016-2383

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



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

The adjust_branches function in kernel/bpf/verifier.c in the Linux kernel before 4.5 does not consider the delta in the backward-jump case, which allows local users to obtain sensitive information from kernel memory by creating a packet filter and then loading crafted BPF instructions.

CVE-2016-2383 has been assigned by security@debian.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
USN-2947-3: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2947-3

USN-2947-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2947-1
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=a1b14d27ed0965838350f1377ff97c93ee383492
oss-security - CVE Request: Linux: Incorrect branch fixups for eBPF allow arbitrary read	www.openwall.com text/html	MLIST [oss-security] 20160214 CVE Request: Linux: Incorrect branch fixups for eBPF allow arbitrary read
USN-2947-2: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2947-2
bpf: fix branch offset adjustment on backjumps after patching ctx exp… · torvalds/linux@a1b14d2 · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/a1b14d27ed0965838350f1377ff97c93ee383492
[security-announce] openSUSE-SU-2016:1008-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1008
Bug 1308452 – CVE-2016-2383 kernel: incorrect branch fixups for eBPG allow arbitrary read	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1308452

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	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	4.5.0	rc1	All	All
Operating System	Linux	Linux Kernel	4.5.0	rc2	All	All
Operating System	Linux	Linux Kernel	4.5.0	rc3	All	All
Operating System	Linux	Linux Kernel	All	rc7	All	All
Operating System	Opensuse	Leap	42.1	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:4.5.0:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:4.5.0:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:4.5.0:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:rc7:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→