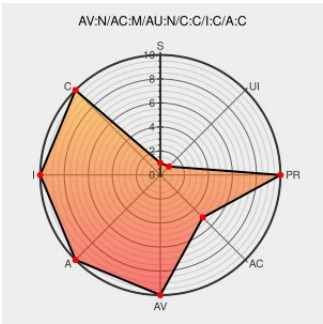
CVE-2015-3331

Published on: 05/27/2015 12:00:00 AM UTC

Last Modified on: 01/19/2023 04:06:00 PM UTC

CVE-2015-3331

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



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

The __driver_rfc4106_decrypt function in arch/x86/crypto/aesni-intel_glue.c in the Linux kernel before 3.19.3 does not properly determine the memory locations used for encrypted data, which allows context-dependent attackers to cause a denial of service (buffer overflow and system crash) or possibly execute arbitrary code by triggering a crypto API call, as demonstrated by use of a libkcapi test program with an AF_ALG(aead) socket.

CVE-2015-3331 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2015:1489-1: important: Live patch for the L	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1489
[security-announce] SUSE-SU-2015:1491-1: important: Live patch for the L	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1491
[security-announce] SUSE-SU-2015:1487-1: important: Live patch for the L	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1487

USN-2631-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2631-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1081
Debian -- Security Information -- DSA-3237-1 linux	www.debian.org Depreciated Link text/html	DEBIAN DSA-3237
oss-security - Buffer overruns in Linux kernel RFC4106 implementation using AESNI	www.openwall.com text/html	MLIST [oss-security] 20150414 Buffer overruns in Linux kernel RFC4106 implementation using AESNI
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ccfe8c3f7e52ae83155cb038753f4c75b774ca8a
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1199
[security-announce] SUSE-SU-2015:1478-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1478
1213322 – (CVE-2015-3331) CVE-2015-3331 Kernel: crypto: buffer overruns in RFC4106 implementation using AESNI	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1213322
Oracle Linux Bulletin - January 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
Linux Kernel __driver_rfc4106_decrypt() Buffer Overflow May Let Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1032416
	Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.19.3
USN-2632-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2632-1
[security-announce] SUSE-SU-2015:1488-1: important: Live patch for the L	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1488
crypto: aesni - fix memory usage in GCM decryption · torvalds/linux@ccfe8c3 · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/ccfe8c3f7e52ae83155cb038753f4c75b774ca8a

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	12.04	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	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:-:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

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→