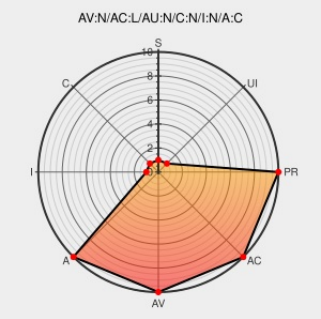
CVE-2014-6417

Published on: 09/28/2014 12:00:00 AM UTC

Last Modified on: 01/19/2023 02:46:00 AM UTC

CVE-2014-6417

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



Certain versions of Linux Kernel from Linux contain the following vulnerability:

net/ceph/auth_x.c in Ceph, as used in the Linux kernel before 3.16.3, does not properly consider the possibility of kmalloc failure, which allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via a long unencrypted auth ticket.

CVE-2014-6417 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
oss-security - Re: CVE Request: libceph auth token overflow / Linux kernel	www.openwall.com text/html	MLIST [oss-security] 20140915 Re: CVE Request: libceph auth token overflow / Linux kernel
Bug 1142072 – CVE-2014-6417 kernel: libceph: incorrect handling of kmalloc failures.	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1142072
USN-2379-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2379-1
libceph: do not hard code max auth ticket len · torvalds/linux@c27a3e4 · GitHub	Exploit github.com text/html	CONFIRM github.com/torvalds/linux/commit/c27a3e4d667fdcad3db7b104f75659478e0c68d8

	Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.16.3
USN-2378-1: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2378-1
Bug #9560: libceph: msg kmalloc failure handling on the reply path - Linux kernel client - Ceph	tracker.ceph.com text/html	CONFIRM tracker.ceph.com/issues/9560
kernel/git/torvalds/linux.git - Linux kernel source tree	Exploit git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=c27a3e4d667fdcad3db7b104f75659478e0c68d8
USN-2376-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2376-1
Bug #8979: GPF kernel panics - auth? - Linux kernel client - Ceph	Exploit tracker.ceph.com text/html	CONFIRM tracker.ceph.com/issues/8979
USN-2377-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2377-1

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	3.16.0	All	All	All
Operating System	Linux	Linux Kernel	3.16.1	All	All	All
Operating System	Linux	Linux Kernel	3.16.0	All	All	All
Operating System	Linux	Linux Kernel	3.16.1	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

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

cpe:2.3:o:linux:linux_kernel:3.16.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.16.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.16.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.16.1:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→