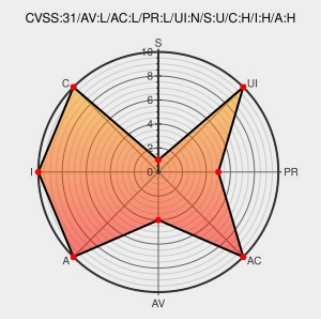
CVE-2012-6701

Published on: 05/02/2016 12:00:00 AM UTC

Last Modified on: 01/17/2023 09:46:00 PM UTC

CVE-2012-6701

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



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

Integer overflow in fs/aio.c in the Linux kernel before 3.4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec.

CVE-2012-6701 has been assigned by security@debian.org 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
1314288 – (CVE-2012-6701) CVE-2012-6701 kernel: AIO interface didn't use rw_verify_area() for checking mandatory locking on files and	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1314288

size of access		
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1854
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=a70b52ec1aaeaf60f4739edb1b422827cb6f3893
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.4.1
vfs: make AIO use the proper rw_verify_area() area helpers · torvalds/linux@a70b52e · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/a70b52ec1aaeaf60f4739edb1b422827cb6f3893
oss-security - Re: CVE Request: Linux: aio write triggers integer overflow in some network protocols	www.openwall.com text/html	MLIST [oss-security] 20160302 Re: CVE Request: Linux: aio write triggers integer overflow in some network protocols

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	All	All	All	All

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→