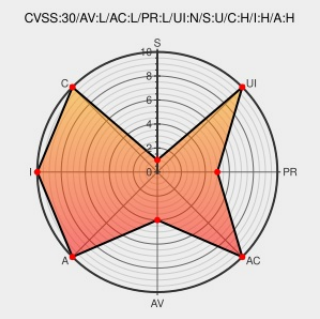
CVE-2015-8830

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

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8830

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



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

Integer overflow in the aio_setup_single_vector function in fs/aio.c in the Linux kernel 4.0 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. NOTE: this vulnerability exists because of a CVE-2012-6701 regression.

CVE-2015-8830 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
USN-2969-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2969-1
Debian -- Security Information -- DSA-3503-1 linux	www.debian.org Depreciated Link	DEBIAN DSA-3503

	text/html	
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1854
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c4f4b82694fe48b02f7a881a1797131a6dad1364
1314275 – (CVE-2015-8830) CVE-2015-8830 kernel: AIO write triggers integer overflow in some protocols	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1314275
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=4c185ce06dca14f5cea192f5a2c981ef50663f2b
USN-2968-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2968-1
aio: lift iov_iter_init() into aio_setup_..._rw() · torvalds/linux@4c185ce · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/4c185ce06dca14f5cea192f5a2c981ef50663f2b
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:3083
USN-2970-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2970-1
USN-2968-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2968-2
AIO: properly check iovec sizes · torvalds/linux@c4f4b82 · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/c4f4b82694fe48b02f7a881a1797131a6dad1364
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
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:3096

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	4.0	All	All	All
Operating System	Linux	Linux Kernel	4.0	All	All	All

cpe:2.3:o:linux:linux_kernel:4.0:*:*:*:*:*:*:*

cpe:2.3:o:linux:linux_kernel:4.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→