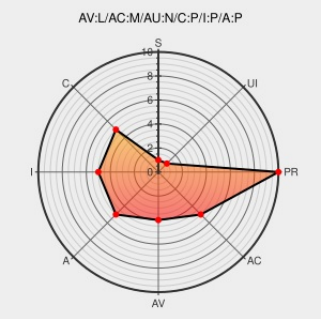
CVE-2015-7312

Published on: 11/16/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7312

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



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

Multiple race conditions in the Advanced Union Filesystem (aufs) aufs3-mmap.patch and aufs4-mmap.patch patches for the Linux kernel 3.x and 4.x allow local users to cause a denial of service (use-after-free and BUG) or possibly gain privileges via a (1) madvise or (2) msync system call, related to mm/madvise.c and mm/msync.c.

CVE-2015-7312 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.4 - MEDIUM

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

CVE References

Description	Tags	Link
oss-security - Re: CVE request: Use-after-free in Linux kernel with aufs mmap patch	Mailing List, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20150922 Re: CVE request: Use-after-free in Linux kernel with aufs mmap patch
USN-2777-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	Third Party Advisory, www.ubuntu.com, text/html	UBUNTU USN-2777-1
Debian -- Security Information -- DSA-3364-1 linux	Third Party Advisory, www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3364
aufs / Re: concurrent msync triggers NULL pointer	Exploit	MLIST [aufs] 20150910 Re: concurrent msync triggers

dereference	Third Party Advisory sourceforge.net text/html	NULL pointer dereference	

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	14.04	All	All	All
Operating System	Debian	Debian Linux	8.0	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:14.04:*:*:*:esm:*:*:*:

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

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

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→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report