



CVE-2016-7118

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-7118
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-31 14:59:00 UTC
Updated	2016-11-28 20:37:00 UTC
Description	fs/fcntl.c in the "aufs 3.2.x+setfl-debian" patch in the linux-image package 3.2.0-4 (kernel 3.2.81-1) in Debian wheezy mishandles the O_APPEND flag, leading to a local denial of service.

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All

References

Reference	Source	Link	Tags
Linux Kernel 'fs/fcntl.c' Local Denial of Service Vulnerability	BID	www.securityfocus.com	
oss-security - Re: CVE request: Kernel Oops when issuing fcntl on an AUFS directory	MLIST	www.openwall.com	Mailing List, T
oss-sec: CVE request: Kernel Oops when issuing fcntl on an AUFS directory	MLIST	seclists.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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