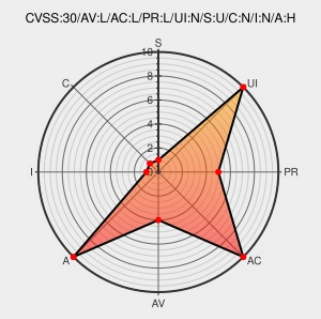
CVE-2017-18257

Published on: 04/04/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18257

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



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

The __get_data_block function in fs/f2fs/data.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow and loop) via crafted use of the open and fallocate system calls with an FS_IOC_FIEMAP ioctl.

CVE-2017-18257 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4188-1 linux	Third Party Advisory, www.debian.org, Depreciated Link, text/html	DEBIAN DSA-4188

USN-3696-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-3696-2
f2fs: fix a dead loop in f2fs_fiemap() · torvalds/linux@b86e330 · GitHub	Patch github.com text/html	MISC github.com/torvalds/linux/commit/b86e33075ed1909d8002745b56ecf73b833db143
USN-3696-1: Linux kernel vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-3696-1
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch git.kernel.org text/html	MISC git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=b86e33075ed1909d8002745b56ecf73b833db143

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	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	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:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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 will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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.

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