

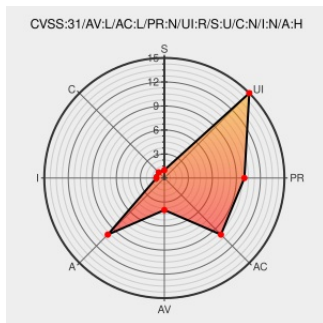


CVE-2018-13096

Published on: 07/03/2018 12:00:00 AM UTC

Last Modified on: 10/07/2022 02:06:00 AM UTC

CVE-2018-13096

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

An issue was discovered in fs/f2fs/super.c in the Linux kernel through 4.14. A denial of service (out-of-bounds memory access and BUG) can occur upon encountering an abnormal bitmap size when mounting a crafted f2fs image.

CVE-2018-13096 has been assigned by [M](#) 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	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
200167 – buffer overrun in build_sit_info() when mounting a crafted f2fs image	Issue Tracking Third Party Advisory bugzilla.kernel.org text/html	MISC bugzilla.kernel.org/show_bug.cgi?id=200167

[SECURITY] [DLA 1715-1] linux-4.9 security update	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20190315 [SECURITY] [DLA 1715-1] linux-4.9 security update
[security-announce] openSUSE-SU-2018:3202-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2018:3202
USN-4118-1: Linux kernel (AWS) vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4118-1
USN-3821-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3821-1
USN-4094-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4094-1
Slackware Security Advisory - Slackware 14.2 kernel Updates ~ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/151420/Slackware-Security-Advisory-Slackware-14.2-kernel-Updates.html
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-030-01)	seclists.org text/html	 BUGTRAQ 20190130 [slackware-security] Slackware 14.2 kernel (SSA:2019-030-01)
USN-3821-2: Linux kernel (Xenial HWE) vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3821-2
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	 MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=e34438c903b653daca2b2a7de95aed46226f8ed3
kernel/git/tip/tip.git - Unnamed repository; edit this file 'description' to name the repository.	git.kernel.org text/html	 CONFIRM git.kernel.org/pub/scm/linux/kernel/git/tip/tip.git/commit/?id=e34438c903b653daca2b2a7de95aed46226f8ed3

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	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	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
Operating System	Opensuse	Leap	42.3	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:14.04.*.*.*:lts:*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04.*.*.*:esm:*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04.*.*.*:lts:*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04.*.*.*:lts:*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04.*.*.*:lts:*.*.*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04.*.*.*:lts:*.*.*:						
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:*.*.*.*.*.*.*:						
cpe:2.3:o:opensuse:leap:42.3.*.*.*.*.*.*:						

No vendor comments have been submitted for this CVE