



CVE-2018-13100

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-13100
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-03 10:29:00 UTC
Updated	2019-04-03 01:29:00 UTC
Description	An issue was discovered in fs/f2fs/super.c in the Linux kernel through 4.17.3, which does not properly validate secs_per_zo

Risk And Classification

Problem Types: CWE-369

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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

References

Reference	Source	Link	Tags
[SECURITY] [DLA 1715-1] linux-4.9 security update	MLIST	lists.debian.org	Third Party Adv
[security-announce] openSUSE-SU-2018:3202-1: important: Security update	SUSE	lists.opensuse.org	
USN-3932-2: Linux kernel (Xenial HWE) vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
Malformed Request	BID	www.securityfocus.com	Third Party Adv
200183 – Divide zero in reset_curseg() when mounting a crafted f2fs image	MISC	bugzilla.kernel.org	Issue Tracking,
USN-3932-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
USN-4118-1: Linux kernel (AWS) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
USN-4094-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
Slackware Security Advisory - Slackware 14.2 kernel Updates ≈ Packet Storm	MISC	packetstormsecurity.com	
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-030-01)	BUGTRAQ	seclists.org	

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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