



# CVE-2018-13099

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-13099
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-07-03 10:29:00 UTC
<b>Updated</b>	2022-10-07 02:08:00 UTC
<b>Description</b>	An issue was discovered in fs/f2fs/inline.c in the Linux kernel through 4.4. A denial of service (out-of-bounds memory access)

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All

## References

Reference	Source	Link	Tag
[SECURITY] [DLA 1531-1] linux-4.9 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mail
[security-announce] openSUSE-SU-2018:3202-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
USN-3932-2: Linux kernel (Xenial HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	

200179 – use-after-free in update_sit_entry() when operating on a corrupted f2fs image	MISC	<a href="https://bugzilla.kernel.org">bugzilla.kernel.org</a>	Expl
USN-3932-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
USN-4118-1: Linux kernel (AWS) vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
USN-4094-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
kernel/git/tip/tip.git - Unnamed repository; edit this file 'description' to name the repository.	CONFIRM	<a href="https://git.kernel.org">git.kernel.org</a>	
Slackware Security Advisory - Slackware 14.2 kernel Updates ~ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-030-01)	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>	
Bugtraq: [SECURITY] [DSA 4308-1] linux security update	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>	
Debian -- Security Information -- DSA-4308-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Thir
Linux Kernel 'fs/f2fs/inline.c' Local Denial of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Thir
linux-f2fs / [f2fs-dev] [PATCH] f2fs: fix to do sanity check with reserved blkaddr of inline inode	MISC	<a href="https://sourceforge.net">sourceforge.net</a>	Patc
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canc
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canc

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)