



CVE-2014-8086

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

Summary

CVE	CVE-2014-8086
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-13 10:55:00 UTC
Updated	2020-08-14 18:16:00 UTC
Description	Race condition in the ext4_file_write_iter function in fs/ext4/file.c in the Linux kernel through 3.17 allows local users to cause a denial of service (kernel panic) and possibly escalate privileges locally.

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party
Linux Kernel 'ext4/file.c' Local Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party
Bug 1151353 – CVE-2014-8086 Kernel: fs: ext4 race condition	CONFIRM	bugzilla.redhat.com	Issue Track
[security-announce] SUSE-SU-2015:1478-1: important: Security update for	SUSE	lists.opensuse.org	Mailing List
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	Third Party
[PATCH] ext4: fix race between write and fcntl(F_SETFL) (Linux Ext4)	MLIST	www.spinics.net	Exploit, Ma
LKML: Dmitry Monakhov: Re: ext4: kernel BUG at fs/ext4/inode.c:2959!	MLIST	lkml.org	Exploit, Ma
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party
LKML:	MLIST	lkml.org	Exploit, Ma
[PATCH] add aio/dio regression test race between write and fcntl V2 (Linux Ext4)	MLIST	www.spinics.net	Mailing List
oss-security - CVE-2014-8086 - Linux kernel ext4 race condition	MLIST	www.openwall.com	Mailing List

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

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