



jbd2: prevent softlockup in jbd2_log_do_checkpoint()

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

Summary

CVE	CVE-2025-39782
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-11 17:15:44 UTC
Updated	2026-05-12 13:17:10 UTC

Description In the Linux kernel, the following vulnerability has been resolved: jbd2: prevent softlockup in jbd2_log_do_checkpoint() Both

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-667

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected f93ea411b73594f7d144855fd34278bcf34a9afc f683d611518d30334813eecf9a8c687453e
CNA	Linux	Linux	affected f93ea411b73594f7d144855fd34278bcf34a9afc f7ee8fd689e6d534f9fd2494b9266f7998082
CNA	Linux	Linux	affected f93ea411b73594f7d144855fd34278bcf34a9afc 84ff98c1ea19acd3f9389e4bb6061364e943
CNA	Linux	Linux	affected f93ea411b73594f7d144855fd34278bcf34a9afc 26cb9aad94cb1811d8fae115594cc71fa3d9
CNA	Linux	Linux	affected f93ea411b73594f7d144855fd34278bcf34a9afc 41f40038de62e8306897cf6840791b26899
CNA	Linux	Linux	affected f93ea411b73594f7d144855fd34278bcf34a9afc 429d50cbaff45090d52a1ea850d5de8c148
CNA	Linux	Linux	affected f93ea411b73594f7d144855fd34278bcf34a9afc 3faac5e1d14c63260fd1bf789d96bde3ab3c
CNA	Linux	Linux	affected f93ea411b73594f7d144855fd34278bcf34a9afc 9d98cf4632258720f18265a058e62fde120c
CNA	Linux	Linux	affected 2.6.16
CNA	Linux	Linux	unaffected 2.6.16 semver
CNA	Linux	Linux	unaffected 5.4.297 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.241 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.190 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.149 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.103 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.44 6.12.* semver
CNA	Linux	Linux	unaffected 6.16.4 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

References

Reference	Source	Link
git.kernel.org/stable/c/26cb9aad94cb1811d8fae115594cc71fa3d91ab0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/84ff98c1ea19acd3f9389e4bb6061364e943f85e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/41f40038de62e8306897cf6840791b268996432a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/3faac5e1d14c63260fd1bf789d96bde3ab3d9e54	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/f683d611518d30334813eecf9a8c687453e2800e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/429d50cbaff45090d52a1ea850d5de8c14881ee7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com

git.kernel.org/stable/c/f7ee8fd689e6d534f9fd2494b9266f7998082e65	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00007.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/9d98cf4632258720f18265a058e62fde120c0151	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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