



jffs2: prevent xattr node from overflowing the eraseblock

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

Summary

CVE	CVE-2024-38599
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-06-19 14:15:19 UTC
Updated	2026-05-12 12:16:54 UTC

Description In the Linux kernel, the following vulnerability has been resolved: jffs2: prevent xattr node from overflowing the eraseblock A

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from nvd@nist.gov

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

Problem Types: CWE-125

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/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 aa98d7cf59b5b0764d3502662053489585faf2fe 2904e1c
CNA	Linux	Linux	affected aa98d7cf59b5b0764d3502662053489585faf2fe 526235c
CNA	Linux	Linux	affected aa98d7cf59b5b0764d3502662053489585faf2fe f0eea09
CNA	Linux	Linux	affected aa98d7cf59b5b0764d3502662053489585faf2fe a1d21bc
CNA	Linux	Linux	affected aa98d7cf59b5b0764d3502662053489585faf2fe f06969c
CNA	Linux	Linux	affected aa98d7cf59b5b0764d3502662053489585faf2fe af82d8c
CNA	Linux	Linux	affected aa98d7cf59b5b0764d3502662053489585faf2fe 8d4313c
CNA	Linux	Linux	affected aa98d7cf59b5b0764d3502662053489585faf2fe 978a12c
CNA	Linux	Linux	affected aa98d7cf59b5b0764d3502662053489585faf2fe c6854e9
CNA	Linux	Linux	affected 2.6.18
CNA	Linux	Linux	unaffected 2.6.18 semver
CNA	Linux	Linux	unaffected 4.19.316 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.278 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.219 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.161 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.93 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.33 6.6.* semver
CNA	Linux	Linux	unaffected 6.8.12 6.8.* semver
CNA	Linux	Linux	unaffected 6.9.3 6.9.* semver
CNA	Linux	Linux	unaffected 6.10 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
git.kernel.org/stable/c/c6854e5a267c28300ff045480b5a7ee7f6f1d913	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/a1d21bcd78cf4a4353e1e835789429c6b76aca8b	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/2904e1d9b64f72d291095e3cbb31634f08788b11	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/f06969df2e40ab1dc8f4364a5de967830c74a098	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/8d431391320c5c5398ff966fb3a95e68a7def275	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org

cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/f0eea095ce8c959b86e1e57fe36ca4fea5ae54f8	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/526235dffcac74c7823ed504dfac4f88d84ba5df	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2024/06/msg00020.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/af82d8d2179b7277ad627c39e7e0778f1c86ccdb	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/978a12c91b38bf1a213e567f3c20e2beef215f07	af854a3a-2127-422b-91ae-364da2661108	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](#) 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](#)