jfs: fix out-of-bounds in dbNextAG() and diAlloc()

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-47723
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 13:15:02 UTC
Updated	2026-05-12 12:17:15 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: jfs: fix out-of-bounds in dbNextAG() and diAlloc() In dbNex

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 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 2.6.12
CNA	Linux	Linux	unaffected 2.6.12 semver
CNA	Linux	Linux	unaffected 4.19.323 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.285 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.227 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.168 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.113 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.54 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.13 6.10.* semver
CNA	Linux	Linux	unaffected 6.11.2 6.11.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	unaffected * custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/03/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/c1ba4b8ca799ff1d99d01f37d7ccb7d5ba5533d2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/96855f40e152989c9e7c20c4691ace5581098acc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/0338e66cba272351ca9d7d03f3628e390e70963b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d1017d2a0f3f16dc1db5120e7ddbe7c6680425b0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/e63866a475562810500ea7f784099bfe341e761a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/128d5cfdcf844cb690c9295a3a1c1114c21fc15a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/5ad6284c8d433f8a213111c5c44ead4d9705b622	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/6ce8b6ab44a8b5918c0ee373d4ad19d19017931b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/ead8253327850242888308 5a787d5a00f15e5eb9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.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.