jfs: Fix uaf in dbFreeBits

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

Summary

CVE	CVE-2024-49903
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 18:15:12 UTC
Updated	2026-05-12 12:17:17 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix uaf in dbFreeBits [syzbot reported] ==========

Risk And Classification

Primary CVSS: v3.1 7 HIGH from nvd@nist.gov

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

Problem Types: CWE-416

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/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 b40c2e665cd552eae5fbdbb878bc29a34357
CNA	Linux	Linux	affected b40c2e665cd552eae5fbdbb878bc29a34357
CNA	Linux	Linux	affected b40c2e665cd552eae5fbdbb878bc29a34357
CNA	Linux	Linux	affected b40c2e665cd552eae5fbdbb878bc29a34357
CNA	Linux	Linux	affected b40c2e665cd552eae5fbdbb878bc29a34357
CNA	Linux	Linux	affected b40c2e665cd552eae5fbdbb878bc29a34357
CNA	Linux	Linux	affected b40c2e665cd552eae5fbdbb878bc29a34357
CNA	Linux	Linux	affected b40c2e665cd552eae5fbdbb878bc29a34357
CNA	Linux	Linux	affected b40c2e665cd552eae5fbdbb878bc29a34357
CNA	Linux	Linux	affected 3.7
CNA	Linux	Linux	unaffected 3.7 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 6.6.55 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.14 6.10.* semver
CNA	Linux	Linux	unaffected 6.11.3 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
git.kernel.org/stable/c/4218b31ecc7af7e191768d32e32ed4386d8f9b76	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/fd026b6b6758d5569705c02540b40f3bbf822b9a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/03/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org

git.kernel.org/stable/c/3126ccde51f51b0648c8cdccaf916e8bd062e972	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.co
git.kernel.org/stable/c/d6c1b3599b2feb5c7291f5ac3a36e5fa7cedb234	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/e7ae14f7ee76c6ef5a48aebab1a278ad78f42619	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/0c238da83f56bb895cab1e5851d034ac45b158d1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/4ac58f7734937f3249da734ede946dfb3b1af5e4	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.co
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/a9603a6f75df2fd8125cd208c98cfaa0fe3f7505	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/95accb7183badca387f7a8d19a2475cf3089f148	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.