



ext4: fix i_data_sem unlock order in ext4_ind_migrate()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2024-50006
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 19:15:04 UTC
Updated	2026-05-12 12:17:19 UTC

Description In the Linux kernel, the following vulnerability has been resolved: ext4: fix i_data_sem unlock order in ext4_ind_migrate() Fu

Risk And Classification

Primary CVSS: v3.1 4.7 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:H/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

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:H/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 e8238f9a8339b3578c85e4192a7a23bc2bdc
CNA	Linux	Linux	affected e8238f9a8339b3578c85e4192a7a23bc2bdc
CNA	Linux	Linux	affected e8238f9a8339b3578c85e4192a7a23bc2bdc
CNA	Linux	Linux	affected e8238f9a8339b3578c85e4192a7a23bc2bdc
CNA	Linux	Linux	affected e8238f9a8339b3578c85e4192a7a23bc2bdc
CNA	Linux	Linux	affected e8238f9a8339b3578c85e4192a7a23bc2bdc
CNA	Linux	Linux	affected e8238f9a8339b3578c85e4192a7a23bc2bdc
CNA	Linux	Linux	affected e8238f9a8339b3578c85e4192a7a23bc2bdc
CNA	Linux	Linux	affected e8238f9a8339b3578c85e4192a7a23bc2bdc
CNA	Linux	Linux	affected 3.10
CNA	Linux	Linux	unaffected 3.10 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	affected V3.2 custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	affected V3.2 custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.2 custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom

References

Reference	Source	Link
cert-portal.siemens.com/productcert/html/ssa-398330.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/6252cb6bde7fc76cb8dcb49d1def7c326b190820	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d43776b907659affef1de888525847d64b244194	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/ef05572da0c0eb89614ed01cc17d3c882bdbd1ff	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/3c46d6060d3e38de22196c1fe7706c5a3c696285	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/53b1999cfd2c7addf2e581a32865fe8835467b44	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/4192adefc9c570698821c5eb9873320eac2fcbf1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/cc749e61c011c255d81b192a822db650c68b313f	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
git.kernel.org/stable/c/9fedf51ab8cf7b69bff08f37fe0989fec7f5d870	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d58a00e981d3118b91d503da263e640b7cde6729	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 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](#)