



scsi: ufs: core: Fix use-after free in init error and remove paths

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

Summary

CVE	CVE-2025-21739
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-02-27 03:15:14 UTC
Updated	2026-04-18 09:16:09 UTC

Description In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix use-after free in init error and remove p

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

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

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/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 d76d9d7d1009968dd3a0fc30e5f5ee9fbffc1350 0dc539b888fb5f56b6eeddd95433eab557d4b0c1 git
CNA	Linux	Linux	affected d76d9d7d1009968dd3a0fc30e5f5ee9fbffc1350 0c77c0d754fe83cb154715fcfec6c3faef94f207 git
CNA	Linux	Linux	affected d76d9d7d1009968dd3a0fc30e5f5ee9fbffc1350 9c185beae09a3eb85f54777edafa227f7e03075d git
CNA	Linux	Linux	affected d76d9d7d1009968dd3a0fc30e5f5ee9fbffc1350 f8fb2403ddebb5eea0033d90d9daae4c88749ada git
CNA	Linux	Linux	affected 5.12
CNA	Linux	Linux	unaffected 5.12 semver
CNA	Linux	Linux	unaffected 6.6.135 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.14 6.12.* semver
CNA	Linux	Linux	unaffected 6.13.3 6.13.* semver
CNA	Linux	Linux	unaffected 6.14 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/f8fb2403ddebb5eea0033d90d9daae4c88749ada	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9c185beae09a3eb85f54777edafa227f7e03075d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/0c77c0d754fe83cb154715fcfec6c3faef94f207	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/0dc539b888fb5f56b6eeddd95433eab557d4b0c1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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