



mfd: core: Add locking around 'mfd_of_node_list'

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

Summary

CVE	CVE-2026-43143
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:31 UTC
Updated	2026-05-13 18:41:04 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: mfd: core: Add locking around 'mfd_of_node_list' Manipulation

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS: 3.1/AV:L/AC:L/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 466a62d7642f02f36d37d9b30c19a725538a01ca dcf679bba02412f2087be21cf06ae88b1f4e0ef git
CNA	Linux	Linux	affected 466a62d7642f02f36d37d9b30c19a725538a01ca e2e7c275f557e2b75e3128f4818063798248774c git
CNA	Linux	Linux	affected 466a62d7642f02f36d37d9b30c19a725538a01ca db131ef9d8980cf60dcac8cf94c036eccf75e5d0 git
CNA	Linux	Linux	affected 466a62d7642f02f36d37d9b30c19a725538a01ca 9b02e3fec3a7fcb990b4d3bd3b13d7edf123dca6 git
CNA	Linux	Linux	affected 466a62d7642f02f36d37d9b30c19a725538a01ca 45341856ecda1d56689451abd5cf1d1aa57dbe47 gi
CNA	Linux	Linux	affected 466a62d7642f02f36d37d9b30c19a725538a01ca 20117c92bcf9c11afd64d7481d8f94fdf410726e git
CNA	Linux	Linux	affected 5.9
CNA	Linux	Linux	unaffected 5.9 semver
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/45341856ecda1d56689451abd5cf1d1aa57dbe47	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9b02e3fec3a7fcb990b4d3bd3b13d7edf123dca6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/db131ef9d8980cf60dcac8cf94c036eccf75e5d0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/e2e7c275f557e2b75e3128f4818063798248774c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/dcf679bba02412f2087be21cf06ae88b1f4e0ef	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/20117c92bcf9c11afd64d7481d8f94fdf410726e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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](#)