



wifi: iwlfwifi: mvm: fix potential out-of-bounds read in iwlmvm_nd_match_info_handler()

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

Summary

CVE	CVE-2026-31779
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 15:16:41 UTC
Updated	2026-05-03 07:16:20 UTC

Description In the Linux kernel, the following vulnerability has been resolved: wifi: iwlfwifi: mvm: fix potential out-of-bounds read in iwlm

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000240000 probability, percentile 0.068220000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	8.1	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
3.1	CNA	DECLARED	8.1	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 5ac54afd4d97ad8d94fe250c83b1924eb6d2268c f6abac936a0dfd31d6c3e49205ec0ee75a8f887f git
CNA	Linux	Linux	affected 5ac54afd4d97ad8d94fe250c83b1924eb6d2268c ffbed27ba15ef80d1c622eedbfef03e501ae134 git
CNA	Linux	Linux	affected 5ac54afd4d97ad8d94fe250c83b1924eb6d2268c e67d8c626ace80b0fa2b48c8ec0a46b508c93442 git
CNA	Linux	Linux	affected 5ac54afd4d97ad8d94fe250c83b1924eb6d2268c dd90880eb5ec5442b37eb2b95688f4a63f4883e3 git
CNA	Linux	Linux	affected 5ac54afd4d97ad8d94fe250c83b1924eb6d2268c ca0e9491b98ca4c5b44204b0b3dd8062a3b5fba2 git
CNA	Linux	Linux	affected 5ac54afd4d97ad8d94fe250c83b1924eb6d2268c 744fab338e87b95c4d1ff7c95bc8c0f834c6d99 git
CNA	Linux	Linux	affected 6.1
CNA	Linux	Linux	unaffected 6.1 semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.134 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/e67d8c626ace80b0fa2b48c8ec0a46b508c93442	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ffbed27ba15ef80d1c622eedbfef03e501ae134	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/744fab338e87b95c4d1ff7c95bc8c0f834c6d99	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ca0e9491b98ca4c5b44204b0b3dd8062a3b5fba2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/dd90880eb5ec5442b37eb2b95688f4a63f4883e3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f6abac936a0dfd31d6c3e49205ec0ee75a8f887f	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.

© [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](#)