



wifi: radiotap: reject radiotap with unknown bits

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

Summary

CVE	CVE-2026-23367
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 11:16:36 UTC
Updated	2026-04-18 09:16:21 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: wifi: radiotap: reject radiotap with unknown bits The radiotap header is used to pass metadata about the captured packet to the user space. The radiotap header is used to pass metadata about the captured packet to the user space. The radiotap header is used to pass metadata about the captured packet to the user space.

Risk And Classification

EPSS: 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 33e5a2f776e331dc8a4379b6efb660d38f182d96 6f80f6a60f5d87e5de5fb2732751fce799991c24 git
CNA	Linux	Linux	affected 33e5a2f776e331dc8a4379b6efb660d38f182d96 d1d1d3c50095928624a95b67a6d7ccc3a18f2215 git
CNA	Linux	Linux	affected 33e5a2f776e331dc8a4379b6efb660d38f182d96 703fa979badbba83d31cd011606d060bfb8b0d1d git
CNA	Linux	Linux	affected 33e5a2f776e331dc8a4379b6efb660d38f182d96 129c8bb320a7cef692c78056ef8e89a2a12ba448 git
CNA	Linux	Linux	affected 33e5a2f776e331dc8a4379b6efb660d38f182d96 2a60c588d5d39ad187628f58395c776a97fd4323 git
CNA	Linux	Linux	affected 33e5a2f776e331dc8a4379b6efb660d38f182d96 2f8ceeba670610d66f77def32011f48de951d781 git
CNA	Linux	Linux	affected 33e5a2f776e331dc8a4379b6efb660d38f182d96 e664971759a0e5570b50c6592e58a7f97d55e992 git
CNA	Linux	Linux	affected 33e5a2f776e331dc8a4379b6efb660d38f182d96 c854758abe0b8d86f9c43dc060ff56a0ee5b31e0 git
CNA	Linux	Linux	affected 2.6.34
CNA	Linux	Linux	unaffected 2.6.34 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.77 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.17 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.7 6.19.* semver

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/6f80f6a60f5d87e5de5fb2732751fce799991c24	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/129c8bb320a7cef692c78056ef8e89a2a12ba448	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/703fa979badbba83d31cd011606d060bfb8b0d1d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d1d1d3c50095928624a95b67a6d7ccc3a18f2215	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2f8ceebea670610d66f77def32011f48de951d781	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2a60c588d5d39ad187628f58395c776a97fd4323	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c854758abe0b8d86f9c43dc060ff56a0ee5b31e0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e664971759a0e5570b50c6592e58a7f97d55e992	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report