



# wifi: wl1251: validate packet IDs before indexing tx\_frames

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

## Summary

<b>CVE</b>	CVE-2026-43113
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 10:16:25 UTC
<b>Updated</b>	2026-05-06 13:07:51 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: wifi: wl1251: validate packet IDs before indexing tx\_frame

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 b6ba1eacf276063ebeeefbbae8056043c24f2efaf git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 df15adc692a802636dd3f258fc7cca8bf7a0ed9a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 8d7465be5163a923ee5d7459719ef5a021c1584a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 26ee518695c484f75e3606d631278e84bd24ae02 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 0fd56fad9c56356e7fa7a7c52e7ecbf807a44eb0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.136 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.83 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.24 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.14 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/0fd56fad9c56356e7fa7a7c52e7ecbf807a44eb0">git.kernel.org/stable/c/0fd56fad9c56356e7fa7a7c52e7ecbf807a44eb0</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/26ee518695c484f75e3606d631278e84bd24ae02">git.kernel.org/stable/c/26ee518695c484f75e3606d631278e84bd24ae02</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/df15adc692a802636dd3f258fc7cca8bf7a0ed9a">git.kernel.org/stable/c/df15adc692a802636dd3f258fc7cca8bf7a0ed9a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/8d7465be5163a923ee5d7459719ef5a021c1584a">git.kernel.org/stable/c/8d7465be5163a923ee5d7459719ef5a021c1584a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/b6ba1eacf276063ebeeefbbae8056043c24f2efaf">git.kernel.org/stable/c/b6ba1eacf276063ebeeefbbae8056043c24f2efaf</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	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](#)