



# net: lan966x: fix page\_pool error handling in lan966x\_fdma\_rx\_alloc\_page\_pool()

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

## Summary

<b>CVE</b>	CVE-2026-31646
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-24 15:16:43 UTC
<b>Updated</b>	2026-04-27 20:19:01 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: net: lan966x: fix page_pool error handling in lan966x_fdm

## 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

**EPSS:** 0.000180000 probability, percentile 0.048130000 (date 2026-04-27)

**Problem Types:** CWE-476

## 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 11871aba19748b3387e83a2db6360aa7119e9a1a e63265f188ea39dcf5f546770650027528f3bd0f git
CNA	Linux	Linux	affected 11871aba19748b3387e83a2db6360aa7119e9a1a 305832c53551cfbe6e5b81ca7ee765e60f4fe8e9 gi
CNA	Linux	Linux	affected 11871aba19748b3387e83a2db6360aa7119e9a1a b5dcb41ba891b55157006cac79825c78a32b409e
CNA	Linux	Linux	affected 11871aba19748b3387e83a2db6360aa7119e9a1a 7caf90d9ab97951a58d1de85ab7e7d7cca7a4513 g
CNA	Linux	Linux	affected 11871aba19748b3387e83a2db6360aa7119e9a1a 3fd0da4fd8851a7e62d009b7db6c4a05b092bc19 g
CNA	Linux	Linux	affected 6.2
CNA	Linux	Linux	unaffected 6.2 semver
CNA	Linux	Linux	unaffected 6.6.135 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.82 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.23 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.13 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/3fd0da4fd8851a7e62d009b7db6c4a05b092bc19	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/7caf90d9ab97951a58d1de85ab7e7d7cca7a4513	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/b5dcb41ba891b55157006cac79825c78a32b409e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/305832c53551cfbe6e5b81ca7ee765e60f4fe8e9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/e63265f188ea39dcf5f546770650027528f3bd0f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</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](#)