



# cxl: Fix race of nvdimm\_bus object when creating nvdimm objects

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

## Summary

<b>CVE</b>	CVE-2026-23348
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-25 11:16:33 UTC
<b>Updated</b>	2026-04-24 18:08:42 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: cxl: Fix race of nvdimm\_bus object when creating nvdimm

## Risk And Classification

**Primary CVSS:** v3.1 4.7 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-362

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:H/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	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8fdbcb1704f61a8fd9be0f3849a174d084def0666 5fc4e150c5ada5f7d20d8f9f1b351f10481fbd7f7 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8fdbcb1704f61a8fd9be0f3849a174d084def0666 5b230daeee420833287cc77314439903e5312f10 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8fdbcb1704f61a8fd9be0f3849a174d084def0666 96a1fd0d84b17360840f344826897fa71049870e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.14
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.14 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.17 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.7 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/5b230daeee420833287cc77314439903e5312f10">git.kernel.org/stable/c/5b230daeee420833287cc77314439903e5312f10</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
<a href="https://git.kernel.org/stable/c/5fc4e150c5ada5f7d20d8f9f1b351f10481fbd7f7">git.kernel.org/stable/c/5fc4e150c5ada5f7d20d8f9f1b351f10481fbd7f7</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
<a href="https://git.kernel.org/stable/c/96a1fd0d84b17360840f344826897fa71049870e">git.kernel.org/stable/c/96a1fd0d84b17360840f344826897fa71049870e</a>	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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)