



# nvdimm/bus: Fix potential use after free in asynchronous initialization

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-31399
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-03 16:16:38 UTC
<b>Updated</b>	2026-04-03 16:16:38 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: nvdimm/bus: Fix potential use after free in asynchronous i

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected b6eae0f61db27748606cc00dafcfd1e2c032f0a5 9a0fb16ba5b372465a3a1ecd761c6fa911a4ab4d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected b6eae0f61db27748606cc00dafcfd1e2c032f0a5 e48bf8f1d2b12c1c5ba1f609edbd4cde5dadc20e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected b6eae0f61db27748606cc00dafcfd1e2c032f0a5 2c638259ad750833fd46a0cf57672a618542d84c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected b6eae0f61db27748606cc00dafcfd1e2c032f0a5 a226e5b49e5fe8c98b14f8507de670189d191348 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected b6eae0f61db27748606cc00dafcfd1e2c032f0a5 84af19855d1abdee3c9d57c0684e2868e391793c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected b6eae0f61db27748606cc00dafcfd1e2c032f0a5 a8aec14230322ed8f1e8042b6d656c1631d41163 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8954771abdea5c34280870e35592c7226a816d95 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3e63a7f25cc85d3d3e174b9b0e3489ebb7eaf4ab git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1490de2bb0836fc0631c04d0559fdf81545b672f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e31a8418c8df7e6771414f99ed3d95ba8aca4e05 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4f1a55a4f990016406147cf3e0c9487bf83e50f0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4.20
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 4.20 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.167 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.130 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.78 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.20 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.10 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0-rc5 * original_commit_for_fix

References				
Reference	Source	Link	Tags	
<a href="https://git.kernel.org/stable/c/a8aec14230322ed8f1e8042b6d656c1631d41163">git.kernel.org/stable/c/a8aec14230322ed8f1e8042b6d656c1631d41163</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/2c638259ad750833fd46a0cf57672a618542d84c">git.kernel.org/stable/c/2c638259ad750833fd46a0cf57672a618542d84c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/a226e5b49e5fe8c98b14f8507de670189d191348">git.kernel.org/stable/c/a226e5b49e5fe8c98b14f8507de670189d191348</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/84af19855d1abdee3c9d57c0684e2868e391793c">git.kernel.org/stable/c/84af19855d1abdee3c9d57c0684e2868e391793c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/9a0fb16ba5b372465a3a1ecd761c6fa911a4ab4d">git.kernel.org/stable/c/9a0fb16ba5b372465a3a1ecd761c6fa911a4ab4d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/e48bf8f1d2b12c1c5ba1f609edbd4cde5dad20e">git.kernel.org/stable/c/e48bf8f1d2b12c1c5ba1f609edbd4cde5dad20e</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	
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](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).

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