



# usb: gadget: f\_tcm: Fix NULL pointer dereferences in nexus handling

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

## Summary

<b>CVE</b>	CVE-2026-43424
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 15:16:54 UTC
<b>Updated</b>	2026-05-12 14:10:27 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f\_tcm: Fix NULL pointer dereferences in nexu

## Risk And Classification

**EPSS:** 0.000240000 probability, percentile 0.070210000 (date 2026-05-11)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c52661d60f636d17e26ad834457db333bd1df494 b9b26d7f3aa288cfa54a7bc68612bab1f153f156 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c52661d60f636d17e26ad834457db333bd1df494 2a2ef846a54a06c33b5c2d4b0d918583e1e7c0b7 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c52661d60f636d17e26ad834457db333bd1df494 d146f27758049fa55ae4c53785a852d3cf7a18d6 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c52661d60f636d17e26ad834457db333bd1df494 f962ca3b020e13d6714f27e8c36fe742441c58d1 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c52661d60f636d17e26ad834457db333bd1df494 679d9535aeb15c10bce89c44102004b96624d706 g
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c52661d60f636d17e26ad834457db333bd1df494 3d309b37633c4a847fc149939a2c9576f1aa1065 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c52661d60f636d17e26ad834457db333bd1df494 b9fde507355342a2d64225d582dc8b98ff5ecb19 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3.5
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 3.5 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.253 5.10.* 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 6.18.19 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.9 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/d146f27758049fa55ae4c53785a852d3cf7a18d6">git.kernel.org/stable/c/d146f27758049fa55ae4c53785a852d3cf7a18d6</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/679d9535aeb15c10bce89c44102004b96624d706">git.kernel.org/stable/c/679d9535aeb15c10bce89c44102004b96624d706</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/b9b26d7f3aa288cfa54a7bc68612bab1f153f156">git.kernel.org/stable/c/b9b26d7f3aa288cfa54a7bc68612bab1f153f156</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/b9fde507355342a2d64225d582dc8b98ff5ecb19">git.kernel.org/stable/c/b9fde507355342a2d64225d582dc8b98ff5ecb19</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/3d309b37633c4a847fc149939a2c9576f1aa1065">git.kernel.org/stable/c/3d309b37633c4a847fc149939a2c9576f1aa1065</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/2a2ef846a54a06c33b5c2d4b0d918583e1e7c0b7">git.kernel.org/stable/c/2a2ef846a54a06c33b5c2d4b0d918583e1e7c0b7</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/f962ca3b020e13d6714f27e8c36fe742441c58d1">git.kernel.org/stable/c/f962ca3b020e13d6714f27e8c36fe742441c58d1</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).

**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)