



# bridge: cfm: Fix race condition in peer\_mep deletion

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

## Summary

<b>CVE</b>	CVE-2026-23393
<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 11:16:40 UTC
<b>Updated</b>	2026-04-02 15:16:33 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: bridge: cfm: Fix race condition in peer\_mep deletion When

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

**EPSS:** 0.000230000 probability, percentile 0.061880000 (date 2026-04-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected dc32cbb3dbd7da38c700d6e0fc6354df24920525 e89dbd2736a45f0507949af4748cbbf3ff793146 git
CNA	Linux	Linux	affected dc32cbb3dbd7da38c700d6e0fc6354df24920525 d8f35767bacb3c7769d470a41cf161e3f3c07e70 git
CNA	Linux	Linux	affected dc32cbb3dbd7da38c700d6e0fc6354df24920525 1fd81151f65927fd9edb8ecd12ad45527dbbe5ab git
CNA	Linux	Linux	affected dc32cbb3dbd7da38c700d6e0fc6354df24920525 3715a00855316066cdda69d43648336367422127 g
CNA	Linux	Linux	affected 5.11
CNA	Linux	Linux	unaffected 5.11 semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.20 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.10 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc5 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/d8f35767bacb3c7769d470a41cf161e3f3c07e70	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/1fd81151f65927fd9edb8ecd12ad45527dbbe5ab	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/e89dbd2736a45f0507949af4748cbbf3ff793146	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/3715a00855316066cdda69d43648336367422127	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/licenses).

