



# net: bridge: fix nd\_tbl NULL dereference when IPv6 is disabled

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

## Summary

<b>CVE</b>	CVE-2026-23381
<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 11:16:38 UTC
<b>Updated</b>	2026-04-18 09:16:22 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: net: bridge: fix nd\_tbl NULL dereference when IPv6 is disabled

## Risk And Classification

**EPSS:** 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ed842faeb2bd49256f00485402f3113205f91d30 a9d712ccfeef737c0e700a4b5b98f310e07b6b60 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ed842faeb2bd49256f00485402f3113205f91d30 a5c56e65b685360dd3f2278aef8c21061feb665 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ed842faeb2bd49256f00485402f3113205f91d30 7a894eb5de246d79f13105c55a67381039a24d44 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ed842faeb2bd49256f00485402f3113205f91d30 a12cdaa3375f0bd3c8f4e564be7c143529abfe5b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ed842faeb2bd49256f00485402f3113205f91d30 aa73deb3b6b730ec280d45b3f423bfa9e17bc122 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ed842faeb2bd49256f00485402f3113205f91d30 33dec6f10777d5a8f71c0a200f690da5ae3c2e55 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ed842faeb2bd49256f00485402f3113205f91d30 20ef5c25422f97dd09d751e5ae6c18406cdc78e6 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ed842faeb2bd49256f00485402f3113205f91d30 e5e890630533bdc15b26a34bb8e7ef539bdf1322 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4.15
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 4.15 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 5.15.203 5.15.* 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 6.12.77 6.12.* 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/a5c56e65b685360dd3f2278aef8c21061feb665">git.kernel.org/stable/c/a5c56e65b685360dd3f2278aef8c21061feb665</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/20ef5c25422f97dd09d751e5ae6c18406cdc78e6">git.kernel.org/stable/c/20ef5c25422f97dd09d751e5ae6c18406cdc78e6</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a12cdaa3375f0bd3c8f4e564be7c143529abfe5b">git.kernel.org/stable/c/a12cdaa3375f0bd3c8f4e564be7c143529abfe5b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/e5e890630533bdc15b26a34bb8e7ef539bdf1322">git.kernel.org/stable/c/e5e890630533bdc15b26a34bb8e7ef539bdf1322</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/7a894eb5de246d79f13105c55a67381039a24d44">git.kernel.org/stable/c/7a894eb5de246d79f13105c55a67381039a24d44</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/33dec6f10777d5a8f71c0a200f690da5ae3c2e55">git.kernel.org/stable/c/33dec6f10777d5a8f71c0a200f690da5ae3c2e55</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a9d712ccfeef737c0e700a4b5b98f310e07b6b60">git.kernel.org/stable/c/a9d712ccfeef737c0e700a4b5b98f310e07b6b60</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/aa73deb3b6b730ec280d45b3f423bfa9e17bc122">git.kernel.org/stable/c/aa73deb3b6b730ec280d45b3f423bfa9e17bc122</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>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

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)