



# netfilter: ip6t\_rt: reject oversized addrnr in rt\_mt6\_check()

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

## Summary

<b>CVE</b>	CVE-2026-31674
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-25 09:16:00 UTC
<b>Updated</b>	2026-04-25 09:16:00 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: netfilter: ip6t_rt: reject oversized addrnr in rt_mt6_check()

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 13e3e30ed3b5b67cc1db2bd58a5d09b0f07debfa git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 af9b7e2b765966457f4ec23be5bd34a141f89574 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 29ea965a1353bc8303877422f79c8211e9ba9c55 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 c6a503a9f4debc654e3a6a7ca1f7fce6a9953c59 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ded71f5684df16fa645cca5bf4fe6b0cd8a46119 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 d8795fde1f78669a87c87ac29fceab2f104daa8c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 a28ebf6f99de270d6338ccdc3b49f3e818f99b7b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 9d3f027327c2fa265f7f85ead41294792c3296ed git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 2.6.12
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 2.6.12 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 6.1.168 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.131 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.80 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.21 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.11 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/d8795fde1f78669a87c87ac29fceab2f104daa8c">git.kernel.org/stable/c/d8795fde1f78669a87c87ac29fceab2f104daa8c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ded71f5684df16fa645cca5bf4fe6b0cd8a46119">git.kernel.org/stable/c/ded71f5684df16fa645cca5bf4fe6b0cd8a46119</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/29ea965a1353bc8303877422f79c8211e9ba9c55">git.kernel.org/stable/c/29ea965a1353bc8303877422f79c8211e9ba9c55</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/13e3e30ed3b5b67cc1db2bd58a5d09b0f07debfa">git.kernel.org/stable/c/13e3e30ed3b5b67cc1db2bd58a5d09b0f07debfa</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9d3f027327c2fa265f7f85ead41294792c3296ed">git.kernel.org/stable/c/9d3f027327c2fa265f7f85ead41294792c3296ed</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a28ebf6f99de270d6338ccdc3b49f3e818f99b7b">git.kernel.org/stable/c/a28ebf6f99de270d6338ccdc3b49f3e818f99b7b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/af9b7e2b765966457f4ec23be5bd34a141f89574">git.kernel.org/stable/c/af9b7e2b765966457f4ec23be5bd34a141f89574</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/c6a503a9f4debc654e3a6a7ca1f7fce6a9953c59">git.kernel.org/stable/c/c6a503a9f4debc654e3a6a7ca1f7fce6a9953c59</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](https://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)