



# batman-adv: avoid OGM aggregation when skb tailroom is insufficient

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

## Summary

<b>CVE</b>	CVE-2026-31683
<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 09:16:02 UTC
<b>Updated</b>	2026-04-25 09:16:02 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: batman-adv: avoid OGM aggregation when skb tailroom is

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c6c8fea29769d998d94fcec9b9f14d4b52b349d3 67176c96f325837b0bb3e9538ca2eba414f447d8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c6c8fea29769d998d94fcec9b9f14d4b52b349d3 0b10a8b355c3f71012ce89289ec2c2f5e3bfd6c1 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c6c8fea29769d998d94fcec9b9f14d4b52b349d3 6755347c5f9bdd44dee80f692208b056fcd40a52 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c6c8fea29769d998d94fcec9b9f14d4b52b349d3 1ada20331f2df2a942d6b83ae1f04a304b642e2a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c6c8fea29769d998d94fcec9b9f14d4b52b349d3 6e40ebb999c2c3d2fbb3cacb61f0384ee6e69075 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c6c8fea29769d998d94fcec9b9f14d4b52b349d3 0e35db29fc5a97a8553f7c2d3a2ba730e46b1ee8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c6c8fea29769d998d94fcec9b9f14d4b52b349d3 eda89a1bae0602aec8314ced299bb243b9f9aeef git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c6c8fea29769d998d94fcec9b9f14d4b52b349d3 0d4aef630be9d5f9c1227d07669c26c4383b5ad0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 2.6.38
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 2.6.38 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 6.12.78 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 * original_commit_for_fix

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/6e40ebb999c2c3d2fbb3cacb61f0384ee6e69075">git.kernel.org/stable/c/6e40ebb999c2c3d2fbb3cacb61f0384ee6e69075</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/1ada20331f2df2a942d6b83ae1f04a304b642e2a">git.kernel.org/stable/c/1ada20331f2df2a942d6b83ae1f04a304b642e2a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/0b10a8b355c3f71012ce89289ec2c2f5e3bfd6c1">git.kernel.org/stable/c/0b10a8b355c3f71012ce89289ec2c2f5e3bfd6c1</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/0e35db29fc5a97a8553f7c2d3a2ba730e46b1ee8">git.kernel.org/stable/c/0e35db29fc5a97a8553f7c2d3a2ba730e46b1ee8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/0d4aef630be9d5f9c1227d07669c26c4383b5ad0">git.kernel.org/stable/c/0d4aef630be9d5f9c1227d07669c26c4383b5ad0</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/eda89a1bae0602aec8314ced299bb243b9f9aeef">git.kernel.org/stable/c/eda89a1bae0602aec8314ced299bb243b9f9aeef</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/67176c96f325837b0bb3e9538ca2eba414f447d8">git.kernel.org/stable/c/67176c96f325837b0bb3e9538ca2eba414f447d8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/6755347c5f9bdd44dee80f692208b056fcd40a52">git.kernel.org/stable/c/6755347c5f9bdd44dee80f692208b056fcd40a52</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)