



# Bluetooth: L2CAP: Fix ERTM re-init and zero pdu\_len infinite loop

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

## Summary

<b>CVE</b>	CVE-2026-31498
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-22 14:16:48 UTC
<b>Updated</b>	2026-04-22 14:16:48 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix ERTM re-init and zero pdu\_len infinite loop

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 96298f640104e4cd9a913a6e50b0b981829b94ff 9760b83cfd24b38caee663f429011a0dd6064fa9 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 96298f640104e4cd9a913a6e50b0b981829b94ff de37e2655b7abc3f59254c6b72256840f39fc6d5 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 96298f640104e4cd9a913a6e50b0b981829b94ff e7aab23b7df89a3d754a5f0a7d2237548b328bd0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 96298f640104e4cd9a913a6e50b0b981829b94ff 52667c859fe33f70c2e711cb81bbd505d5eb8e75 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 96298f640104e4cd9a913a6e50b0b981829b94ff 9a21a631ee034b1573dce14b572a24943dbfd7ae git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 96298f640104e4cd9a913a6e50b0b981829b94ff 900e4db5385ec2cacd372345a80ab9c8e105b3a3 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 96298f640104e4cd9a913a6e50b0b981829b94ff 042e2cd4bb11e5313b19b87593616524949e4c52 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 96298f640104e4cd9a913a6e50b0b981829b94ff 25f420a0d4cfd61d3d23ec4b9c56d9f443d91377 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4ad03ff6f680681c5f78254e37c4c856fa953629 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected b7d0ca715c1008acd2fc018f02a56fed88f78b75 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 799263eb37a4f7f6d39334046929c3bc92452a7f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8828622fb9b4201eeb0870587052e3d834cfaf61 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected b432ea85ab8472763870dd0f2c186130dd36d68c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.7
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.7 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/25f420a0d4cfd61d3d23ec4b9c56d9f443d91377">git.kernel.org/stable/c/25f420a0d4cfd61d3d23ec4b9c56d9f443d91377</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/900e4db5385ec2cacd372345a80ab9c8e105b3a3">git.kernel.org/stable/c/900e4db5385ec2cacd372345a80ab9c8e105b3a3</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/de37e2655b7abc3f59254c6b72256840f39fc6d5">git.kernel.org/stable/c/de37e2655b7abc3f59254c6b72256840f39fc6d5</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9760b83cfd24b38caee663f429011a0dd6064fa9">git.kernel.org/stable/c/9760b83cfd24b38caee663f429011a0dd6064fa9</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/042e2cd4bb11e5313b19b87593616524949e4c52">git.kernel.org/stable/c/042e2cd4bb11e5313b19b87593616524949e4c52</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9a21a631ee034b1573dce14b572a24943dbfd7ae">git.kernel.org/stable/c/9a21a631ee034b1573dce14b572a24943dbfd7ae</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/e7aab23b7df89a3d754a5f0a7d2237548b328bd0">git.kernel.org/stable/c/e7aab23b7df89a3d754a5f0a7d2237548b328bd0</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/52667c859fe33f70c2e711cb81bbd505d5eb8e75">git.kernel.org/stable/c/52667c859fe33f70c2e711cb81bbd505d5eb8e75</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](#) 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)