



# Bluetooth: L2CAP: Fix null-ptr-deref on l2cap\_sock\_ready\_cb

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

## Summary

<b>CVE</b>	CVE-2026-31510
<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 14:16:50 UTC
<b>Updated</b>	2026-04-22 14:16:50 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix null-ptr-deref on l2cap\_sock\_ready\_cb

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 54a59aa2b562872781d6a8fc89f300d360941691 d34776c7fa1f2c510f1cdd14823aba701babb4ad git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 54a59aa2b562872781d6a8fc89f300d360941691 03d4eafb0f3788239df63575951f6b4c97bbfda4 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 54a59aa2b562872781d6a8fc89f300d360941691 3c821bc0fbeaa27910a20d0b43c6008d099792af git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 54a59aa2b562872781d6a8fc89f300d360941691 a04a760c06bb591989db659439efdf106f0bae76 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 54a59aa2b562872781d6a8fc89f300d360941691 0780f9333852971ca77d110019e3a66ce5a7b100 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 54a59aa2b562872781d6a8fc89f300d360941691 1dc6db047919ecd59493cd51248b37381bbabcb g
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 54a59aa2b562872781d6a8fc89f300d360941691 898b89c90ff9496e64b9331040778cc4e1b28c9d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 54a59aa2b562872781d6a8fc89f300d360941691 b6552e0503973daf6f23bd6ed9273ef131ee364f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3.6
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 3.6 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/b6552e0503973daf6f23bd6ed9273ef131ee364f">git.kernel.org/stable/c/b6552e0503973daf6f23bd6ed9273ef131ee364f</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/03d4eafb0f3788239df63575951f6b4c97bbfda4">git.kernel.org/stable/c/03d4eafb0f3788239df63575951f6b4c97bbfda4</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a04a760c06bb591989db659439efdf106f0bae76">git.kernel.org/stable/c/a04a760c06bb591989db659439efdf106f0bae76</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/1dc6db047919ecd59493cd51248b37381bbabcbb">git.kernel.org/stable/c/1dc6db047919ecd59493cd51248b37381bbabcbb</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/0780f9333852971ca77d110019e3a66ce5a7b100">git.kernel.org/stable/c/0780f9333852971ca77d110019e3a66ce5a7b100</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/898b89c90ff9496e64b9331040778cc4e1b28c9d">git.kernel.org/stable/c/898b89c90ff9496e64b9331040778cc4e1b28c9d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/d34776c7fa1f2c510f1cdd14823aba701babb4ad">git.kernel.org/stable/c/d34776c7fa1f2c510f1cdd14823aba701babb4ad</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/3c821bc0fbeaa27910a20d0b43c6008d099792af">git.kernel.org/stable/c/3c821bc0fbeaa27910a20d0b43c6008d099792af</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](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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://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)