



# Bluetooth: L2CAP: Fix stack-out-of-bounds read in l2cap\_ecred\_conn\_req

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

## Summary

<b>CVE</b>	CVE-2026-31513
<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 stack-out-of-bounds read in l2cap\_

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 935f324e4b2461df2cf7f02b4195082b4304c708 c8e1a27edb8b4e5afb56b384acd7b6c2dec1b7cc git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e981a9392800ce2c5bca196a6ab2c55e9370efaa 5b35f8211a913cfe7ab9d54fa36a272d2059a588 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f3fd2e7276a3edc5df55454275da20eac186970 a3d9c50d69785ae02e153f000da1b5fd6dbfdf1b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c28d2bff70444a85b3b86aaf241ece9408c7858c 9d87cb22195b2c67405f5485d525190747ad5493 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.12.75 6.12.80 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.18.16 6.18.21 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.19.6 6.19.11 semver

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/c8e1a27edb8b4e5afb56b384acd7b6c2dec1b7cc">git.kernel.org/stable/c/c8e1a27edb8b4e5afb56b384acd7b6c2dec1b7cc</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/5b35f8211a913cfe7ab9d54fa36a272d2059a588">git.kernel.org/stable/c/5b35f8211a913cfe7ab9d54fa36a272d2059a588</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a3d9c50d69785ae02e153f000da1b5fd6dbfdf1b">git.kernel.org/stable/c/a3d9c50d69785ae02e153f000da1b5fd6dbfdf1b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9d87cb22195b2c67405f5485d525190747ad5493">git.kernel.org/stable/c/9d87cb22195b2c67405f5485d525190747ad5493</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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)