# Bluetooth: hci_sync: fix stack buffer overflow in hci_le_big_create_sync

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-31772 |
| **State** | PUBLISHED |
| **Assigner** | Linux |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-05-01 15:16:40 UTC |
| **Updated** | 2026-05-03 07:16:20 UTC |
| **Description** | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: fix stack buffer overflow in hci_le_big |

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**EPSS:** 0.000180000 probability, percentile 0.046600000 (date 2026-05-02)

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | Secondary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | CNA | DECLARED | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|---|---|---|---|
| CNA | Linux | Linux | affected 91d19383b7ed035e22165ae5c836e50bb9f95fbe f5d446624345d309e7a4a1b27ea9f028d6a8c5d9 git |
| CNA | Linux | Linux | affected 42ecf1947135110ea08abeaca39741636f9a2285 aba0aea354015794e8312dd7efe726967e58aefe git |
| CNA | Linux | Linux | affected 42ecf1947135110ea08abeaca39741636f9a2285 eaf32002ca7b1ba51c9f140991fd9febe6de79f0 git |
| CNA | Linux | Linux | affected 42ecf1947135110ea08abeaca39741636f9a2285 bc39a094730ce062fa034a529c93147c096cb488 git |
| CNA | Linux | Linux | affected 8958e1cee4e2eac1a5b825caa4dd96ce9ed975dd git |
| CNA | Linux | Linux | affected 6.13 |
| CNA | Linux | Linux | unaffected 6.13 semver |
| CNA | Linux | Linux | unaffected 6.12.81 6.12.* semver |
| CNA | Linux | Linux | unaffected 6.18.22 6.18.* semver |
| CNA | Linux | Linux | unaffected 6.19.12 6.19.* semver |
| CNA | Linux | Linux | unaffected 7.0 * original_commit_for_fix |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| git.kernel.org/stable/c/aba0aea354015794e8312dd7efe726967e58aefe | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/f5d446624345d309e7a4a1b27ea9f028d6a8c5d9 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/bc39a094730ce062fa034a529c93147c096cb488 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/eaf32002ca7b1ba51c9f140991fd9febe6de79f0 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonica |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonica |

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 registred 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**