# CVE-2011-2497

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2011-2497 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2011-08-29 18:55:00 UTC |
| **Updated** | 2023-02-13 01:19:00 UTC |
| **Description** | Integer underflow in the l2cap_config_req function in net/bluetooth/l2cap_core.c in the Linux kernel before 3.0 allows remot |

## Risk And Classification

**Problem Types:** CWE-191

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| Bluetooth: Prevent buffer overflow in l2cap config request - CXSecurity.com | SREASON | securityreason.com | Patch, Third |
| kernel/git/torvalds/linux.git - Linux kernel source tree | CONFIRM | git.kernel.org | Patch, Vend |
| 404: File not found | CONFIRM | www.kernel.org | Broken Link |
| Linux kernel l2cap Remote Buffer Overflow Vulnerability | BID | www.securityfocus.com | Third Party |
| '[PATCH] Bluetooth: Prevent buffer overflow in l2cap config request' - MARC | MLIST | marc.info | Patch, Third |
| oss-security - CVE request: kernel: remote buffer overflow in bluetooth | MLIST | www.openwall.com | Mailing List |
| Red Hat Customer Portal | MISC | access.redhat.com | |
| Bug 716805 – CVE-2011-2497 kernel: bluetooth: buffer overflow in l2cap config request | CONFIRM | bugzilla.redhat.com | Issue Track |
| oss-security - Re: CVE request: kernel: remote buffer overflow in bluetooth | MLIST | www.openwall.com | Mailing List |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC | git.kernel.org | |
| Red Hat Customer Portal | MISC | access.redhat.com | |
| 74679 | OSVDB | www.osvdb.org | Broken Link |

| | | | |
|---|---|---|---|
| access.redhat.com \| CVE-2011-2497 | MISC | access.redhat.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, a |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.