# CVE-2011-4060

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2011-4060 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2011-10-18 01:55:01 UTC |
| **Updated** | 2026-04-29 01:13:23 UTC |
| **Description** | The runtime linker in QNX Neutrino RTOS 6.5.0 before Service Pack 1 does not properly clear the LD_DEBUG_OUTPUT a |

## Risk And Classification

**Primary CVSS:** v2.0 3.3 from nvd@nist.gov

AV:L/AC:M/Au:N/C:N/I:P/A:P

**Problem Types:** CWE-59 | n/a

### CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

Partial

AV:L/AC:M/Au:N/C:N/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Qnx | Neutrino Rtos | 6.5.0 | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Na | N/a | affected n/a | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| Help - Eclipse SDK | af854a3a-2127-422b-91ae-364da2661108 | www.qnx |
| Embedded Systems Software Platform \| BlackBerry QNX | af854a3a-2127-422b-91ae-364da2661108 | www.qnx |
| SecurityFocus | af854a3a-2127-422b-91ae-364da2661108 | www.sec |
| www.osvdb.org/71784 | af854a3a-2127-422b-91ae-364da2661108 | www.osv |
| www.nth-dimension.org.uk/pub/NDSA20110310.txt.asc | af854a3a-2127-422b-91ae-364da2661108 | www.nth- |
| QNX Neutrino RTOS 'LD_DEBUG_OUTPUT' Local Privilege Escalation Vulnerability | af854a3a-2127-422b-91ae-364da2661108 | www.sec |
| SecurityFocus | af854a3a-2127-422b-91ae-364da2661108 | www.sec |
| CXSecurity - IDS | af854a3a-2127-422b-91ae-364da2661108 | securityre |
| CVE Program record | CVE.ORG | www.cve |
| NVD vulnerability detail | NVD | nvd.nist.g |

No vendor comments have been submitted for this CVE.

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