# CVE-2016-8650

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-8650 |
| **State** | PUBLISHED |
| **Assigner** | redhat |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2016-11-28 03:59:09 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | The mpi_powm function in lib/mpi/mpi-pow.c in the Linux kernel through 4.8.11 does not ensure that memory is allocated fo |

## Risk And Classification

**Primary CVSS:** v3.0 5.5 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

**EPSS:** 0.000450000 probability, percentile 0.136460000 (date 2026-05-07)

**Problem Types:** CWE-20 | CWE-399 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.0 | nvd@nist.gov | Primary | 5.5 | MEDIUM | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H |
| 2.0 | nvd@nist.gov | Primary | 4.9 | | AV:L/AC:L/Au:N/C:N/I:N/A:C |

## CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

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

## Vendor Declared Affected Products

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

## References

| Reference |
|---|
| Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remote Users |
| Full Disclosure: OS-S 2016-21 - Local DoS: Linux Kernel Nullpointer Dereference via keyctl |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| kernel/git/torvalds/linux.git - Linux kernel source tree |
| oss-security - Linux kernel: CVE-2016-8650 : Local denial of service with in key subsystem |
| Linux Kernel CVE-2016-8650 Null Pointer Deference Local Denial of Service Vulnerability |
| Bug 1395187 – CVE-2016-8650 kernel: Null pointer dereference via keyctl |

| |
|---|
| Bug [illegible] CVE-2016-8650 kernel: Null pointer dereference via keyctl |
| mpi: Fix NULL ptr dereference in mpi_powm() [ver #3] · torvalds/linux@f5527ff · GitHub |
| Android Security Bulletin—March 2017 \| Android Open Source Project |
| Red Hat Customer Portal |
| CVE-2016-8650 - Red Hat Customer Portal |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

378168 Virtuozzo Linux Security Update for perf (VZLSA-2017:0933)