



# CVE-2016-8630

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

## Summary

|                 |                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-8630                                                                                                            |
| State           | PUBLISHED                                                                                                                |
| Assigner        | redhat                                                                                                                   |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                             |
| Published       | 2016-11-28 03:59:03 UTC                                                                                                  |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                                  |
| Description     | The x86_decode_insn function in arch/x86/kvm/emulate.c in the Linux kernel before 4.8.7, when KVM is enabled, allows loc |

## 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:** 0.000310000 probability, percentile 0.088880000 (date 2026-05-10)

**Problem Types:** CWE-284 | CWE-476 | 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                                                                                         | Source                          |
|---------------------------------------------------------------------------------------------------|---------------------------------|
| Red Hat Customer Portal                                                                           | af854a3a-2127-422b-91ae-364da26 |
| kernel/git/torvalds/linux.git - Linux kernel source tree                                          | af854a3a-2127-422b-91ae-364da26 |
| Linux Kernel 'kvm/emulate.c' Null Pointer Dereference Denial of Service Vulnerability             | af854a3a-2127-422b-91ae-364da26 |
| oss-security - CVE-2016-8630 kernel: kvm: x86: NULL pointer dereference during instruction decode | af854a3a-2127-422b-91ae-364da26 |
| kvm: x86: Check memopp before dereference (CVE-2016-8630) · torvalds/linux@d9092f5 · GitHub       | af854a3a-2127-422b-91ae-364da26 |
| Red Hat Customer Portal                                                                           | af854a3a-2127-422b-91ae-364da26 |
| Bug 1393350 – CVE-2016-8630 kernel: kvm: x86: NULL pointer dereference during instruction decode  | af854a3a-2127-422b-91ae-364da26 |
| www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.8.7                                              | af854a3a-2127-422b-91ae-364da26 |
| Red Hat Customer Portal                                                                           | MITRF                           |

|                                                                                |         |
|--------------------------------------------------------------------------------|---------|
| Red Hat Customer Portal                                                        | MITRE   |
| CVE-2016-8630 - Red Hat Customer Portal                                        | MITRE   |
| CVE Program record                                                             | CVE.ORG |
| NVD vulnerability detail                                                       | NVD     |
| No vendor comments have been submitted for this CVE.                           |         |
| Legacy QID Mappings                                                            |         |
| 378284 Virtuozzo Linux Security Update for kernel-tools-libs (VZLSA-2017:0386) |         |

© [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](#)