# CVE-2016-1568

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-1568 |
| **State** | PUBLISHED |
| **Assigner** | redhat |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2016-04-12 02:00:05 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | Use-after-free vulnerability in hw/ide/ahci.c in QEMU, when built with IDE AHCI Emulation support, allows guest OS users t |

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

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

**Problem Types:** CWE-416 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | nvd@nist.gov | Primary | 8.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H |
| 2.0 | nvd@nist.gov | Primary | 6.9 | | AV:L/AC:M/Au:N/C:C/I:C/A:C |

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Application | Redhat | Openstack | 5.0 | All | All | All |
| Application | Redhat | Openstack | 6.0 | All | All | All |
| Application | Redhat | Openstack | 7.0 | All | All | All |
| Application | Redhat | Virtualization | 3.0 | All | All | All |

## Vendor Declared Affected Products

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

## References

| Reference |
|---|
| Debian -- Security Information -- DSA-3469-1 qemu |
| Red Hat Customer Portal |
| git.qemu.org Git - qemu.git/commit |

| |
|---|
| Debian -- Security Information -- DSA-3470-1 qemu-kvm |
| QEMU AHCI NCQ AIO Command Processing Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTra |
| Red Hat Customer Portal |
| Debian -- Security Information -- DSA-3471-1 qemu |
| QEMU CVE-2016-1568 Remote Code Execution Vulnerability |
| oss-security - Qemu: ide: ahci use-after-free vulnerability in aio port commands |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| QEMU: Multiple vulnerabilities (GLSA 201602-01) — Gentoo security |
| oss-security - Re: Qemu: ide: ahci use-after-free vulnerability in aio port commands |
| git.qemu.org Git - qemu.git/commit |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| CVE-2016-1568 - Red Hat Customer Portal |
| 1288532 – (CVE-2016-1568) CVE-2016-1568 Qemu: ide: ahci use-after-free vulnerability in aio port commands |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

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