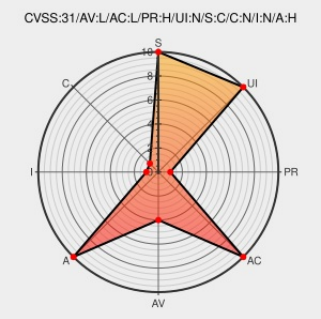
# CVE-2016-5107

Published on: 09/02/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:06:58 PM UTC

## CVE-2016-5107

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The megasas_lookup_frame function in QEMU, when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds read and crash) via unspecified vectors.

CVE-2016-5107 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 6 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| LOCAL | LOW | HIGH | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| CHANGED | NONE | NONE | HIGH |

### CVSS2 Score: 1.9 - LOW

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| [SECURITY] [DLA 1599-1] qemu security update | Mailing List, Third Party Advisory, lists.debian.org, text/html | MLIST [debian-lts-announce] 20181130 [SECURITY] [DLA 1599-1] qemu security update |

| | | |
|---|---|---|
| oss-security - Re: CVE Request Qemu: scsi: megasas: out-of-bounds read in megasas_lookup_frame() function | Mailing List<br>Third Party Advisory<br>www.openwall.com<br>text/html | MLIST [oss-security] 20160526 Re: CVE Request Qemu: scsi: megasas: out-of-bounds read in megasas_lookup_frame() function |
| [Qemu-devel] [PATCH v2] scsi: megasas: check 'read_queue_head' index val | Mailing List<br>Patch<br>Third Party Advisory<br>lists.gnu.org<br>text/x-diff | MLIST [qemu-devel] 20160525 [Qemu-devel] [PATCH v2] scsi: megasas: check 'read_queue_head' index val |
| USN-3047-1: QEMU vulnerabilities \| Ubuntu | Third Party Advisory<br>www.ubuntu.com<br>text/html | UBUNTU USN-3047-1 |
| QEMU 'megasas_lookup_frame()' Function Out of Bounds Read Denial of Service Vulnerability | Third Party Advisory<br>VDB Entry<br>cve.report (archive)<br>text/html | BID 90874 |
| USN-3047-2: QEMU regression \| Ubuntu | Third Party Advisory<br>www.ubuntu.com<br>text/html | UBUNTU USN-3047-2 |
| Bug 1336461 – CVE-2016-5107 Qemu: scsi: megasas: out-of-bounds read in megasas_lookup_frame() function | Issue Tracking<br>Third Party Advisory<br>bugzilla.redhat.com<br>text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1336461 |
| oss-security - CVE Request Qemu: scsi: megasas: out-of-bounds read in megasas_lookup_frame() function | Mailing List<br>Third Party Advisory<br>www.openwall.com<br>text/html | MLIST [oss-security] 20160525 CVE Request Qemu: scsi: megasas: out-of-bounds read in megasas_lookup_frame() function |
| QEMU: Multiple vulnerabilities (GLSA 201609-01) — Gentoo security | Third Party Advisory<br>security.gentoo.org<br>text/html | GENTOO GLSA-201609-01 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→