



CVE-2016-9915

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2016-9915 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2016-12-29 22:59:00 UTC |
| Updated | 2023-02-12 23:27:00 UTC |
| Description | Memory leak in hw/9pfs/9p-handle.c in QEMU (aka Quick Emulator) allows local privileged guest OS users to cause a denial of service. |

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Qemu | Qemu | 2.8.0 | rc0 | All | All |
| Application | Qemu | Qemu | 2.8.0 | rc1 | All | All |
| Application | Qemu | Qemu | 2.8.0 | rc0 | All | All |
| Application | Qemu | Qemu | 2.8.0 | rc1 | All | All |
| Application | Qemu | Qemu | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|---|---------------|
| QEMU: Multiple vulnerabilities (GLSA 201701-49) — Gentoo security | GENTOO | security.gentoo.org | Third Party |
| [SECURITY] [DLA 1497-1] qemu security update | MLIST | lists.debian.org | Third Party |
| git.qemu.org Git - qemu.git/commit | MISC | git.qemu.org | |
| [Qemu-devel] [PATCH v3 0/4] 9pfs: add cleanup operation in handle/proxy | MLIST | lists.gnu.org | Patch, Vendor |
| QEMU VirtFS Multiple Denial of Service Vulnerabilities | BID | www.securityfocus.com | Third Party |
| git.qemu.org Git - qemu.git/commit | CONFIRM | git.qemu.org | Issue Track |
| oss-security - Re: CVE request Qemu: 9pfs: memory leakage via proxy/handle callbacks | MLIST | www.openwall.com | Mailing List |

| | | | |
|--|---------|--|--------------|
| oss-security - CVE request Qemu: 9pfs: memory leakage via proxy/handle callbacks | MLIST | www.openwall.com | Mailing List |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, c |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710389](#) Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201701-49)

[900063](#) CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

© [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](#).

CVE.report and Source URL Uptime Status status.cve.report