



CVE-2020-1711

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-1711 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-02-11 20:15:00 UTC |
| Updated | 2023-11-07 03:19:00 UTC |
| Description | An out-of-bounds heap buffer access flaw was found in the way the iSCSI Block driver in QEMU versions 2.12.0 before 4.2 |

Risk And Classification

Problem Types: CWE-787

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 | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |
| Application | Redhat | Openstack | 10 | All | All | All |
| Application | Redhat | Openstack | 13 | All | All | All |
| Application | Redhat | Openstack | 13.0 | All | All | All |
| Application | Redhat | Openstack | 10 | All | All | All |
| Application | Redhat | Openstack | 13.0 | All | All | All |

References

| Reference | Source |
|--|--------|
| [PATCH] iscsi: Cap block count from GET LBA STATUS (CVE-2020-1711) | MISC |
| Red Hat Customer Portal | REDHAT |
| QEMU: Multiple vulnerabilities (GLSA 202005-02) — Gentoo security | GENTOO |
| USN-4283-1: QEMU vulnerabilities Ubuntu security notices Ubuntu | UBUNTU |
| oss-security - CVE-2020-1711 QEMU: block: iscsi: OOB heap access via an unexpected response of iSCSI Server | MISC |
| Red Hat Customer Portal | REDHAT |
| Red Hat Customer Portal | REDHAT |
| 1794290 – (CVE-2020-1711) CVE-2020-1711 QEMU: block: iscsi: OOB heap access via an unexpected response of iSCSI Server | CONFIR |
| [SECURITY] [DLA 2144-1] qemu security update | MLIST |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | REDHAT |
| [SECURITY] [DLA 2373-1] qemu security update | MLIST |
| [security-announce] openSUSE-SU-2020:0468-1: important: Security update | SUSE |
| CVE Program record | CVE.OP |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 377413 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)
- 900050 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
- 903618 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1959)
- 940144 AlmaLinux Security Update for virt:rhel (ALSA-2020:1358)
- 960718 Rocky Linux Security Update for virt:rhel (RLSA-2020:1358)

© 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](#)