



CVE-2020-14364

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2020-14364 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-08-31 18:15:00 UTC |
| Updated | 2023-11-07 03:17:00 UTC |
| Description | An out-of-bounds read/write access flaw was found in the USB emulator of the QEMU in versions before 5.2.0. This issue c |

Risk And Classification

Problem Types: CWE-125 | CWE-787

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|----------------------------------|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 20.04 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Opensuse | Leap | 15.2 | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 6.0 | 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 | 8.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 6.0 | 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 | 8.0 | All | All | All |
| Application | Redhat | Openstack | 10 | All | All | All |
| Application | Redhat | Openstack | 13 | All | All | All |
| Application | Redhat | Openstack | 10 | All | All | All |
| Application | Redhat | Openstack | 13 | All | All | All |

References

| Reference | Source | Link |
|--|---------|---------------------|
| 1869201 – (CVE-2020-14364) CVE-2020-14364 QEMU: usb: out-of-bounds r/w access issue while processing usb packets | MISC | bu |
| [SECURITY] Fedora 32 Update: xen-4.13.1-5.fc32 - package-announce - Fedora Mailing-Lists | | lis |
| [SECURITY] Fedora 31 Update: xen-4.12.3-4.fc31 - package-announce - Fedora Mailing-Lists | FEDORA | lis |
| [security-announce] openSUSE-SU-2020:1664-1: important: Security update | SUSE | lis |
| [SECURITY] Fedora 32 Update: xen-4.13.1-5.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | lis |
| Debian -- Security Information -- DSA-4760-1 qemu | DEBIAN | wv |
| USN-4511-1: QEMU vulnerability Ubuntu security notices Ubuntu | UBUNTU | us |
| QEMU: Multiple vulnerabilities (GLSA 202011-09) — Gentoo security | GENTOO | se |
| oss-security - CVE-2020-14364 QEMU: usb: out-of-bounds r/w access issue while processing usb packets | MISC | wv |
| oss-security - Xen Security Advisory 335 v2 (CVE-2020-14364) - QEMU: usb: out-of-bounds r/w access issue | MISC | wv |
| Xen: Buffer overflow (GLSA 202009-14) — Gentoo security | GENTOO | se |
| [SECURITY] Fedora 31 Update: xen-4.12.3-4.fc31 - package-announce - Fedora Mailing-Lists | | lis |
| [SECURITY] [DLA 2373-1] qemu security update | MLIST | lis |
| CVE-2020-14364 QEMU Vulnerability in NetApp Products NetApp Product Security | CONFIRM | se |
| CVE Program record | CVE.ORG | wv |
| NVD vulnerability detail | NVD | nv |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[174921](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)

[174922](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1240-1)

[174923](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)

[174924](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)

| |
|---|
| 375439 Citrix XenServer Security Updates (CTX280451) |
| 377046 Alibaba Cloud Linux Security Update for qemu-kvm-ma (ALINUX2-SA-2020:0117) |
| 377063 Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2020:0120) |
| 377413 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119) |
| 378320 Virtuozzo Linux Security Update for qemu-img (VZLSA-2020:4056) |
| 500791 Alpine Linux Security Update for xen |
| 501230 Alpine Linux Security Update for qemu |
| 501511 Alpine Linux Security Update for xen |
| 501682 Alpine Linux Security Update for qemu |
| 502352 Alpine Linux Security Update for qemu |
| 504535 Alpine Linux Security Update for xen |
| 750097 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1837-1) |
| 750120 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1893-1) |
| 750124 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1894-1) |
| 750129 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1895-1) |
| 750138 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1918-1) |
| 750149 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1942-1) |
| 750152 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1947-1) |
| 750771 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1942-1) |
| 750827 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1043-1) |
| 900187 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0 |
| 903250 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (2027) |
| 940244 AlmaLinux Security Update for virt:rhel (ALSA-2020:4059) |
| 960682 Rocky Linux Security Update for virt:rhel (RLSA-2020:4059) |

© [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](#).

