



# CVE-2021-20196

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-20196  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert@redhat.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2021-05-26 22:15:00 UTC   |
| <b>Updated</b>         | 2023-02-12 22:15:00 UTC   |
| <b>Description</b>     | A NULL pointer dereference flaw was found in the floppy disk emulator of QEMU. This issue occurs while processing read/ |

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                      | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Application      | <a href="#">Qemu</a>   | <a href="#">Qemu</a>         | 5.2.0   | -      | All     | All      |

## References

| Reference  | Source  | Link                       |
|--|---------|----------------------------|
| 1919210 – (CVE-2021-20196) CVE-2021-20196 QEMU: block: fdc: null pointer dereference may lead to guest crash | MISC    | <a href="#">bugzilla.r</a> |
| [SECURITY] [DLA 3099-1] qemu security update   | MLIST   | <a href="#">lists.debi</a> |
| Bug #1912780 "QEMU: Null Pointer Failure in fdctrl_read() in hw/..." : Bugs : QEMU                           | MISC    | <a href="#">bugs.laur</a>  |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC    | <a href="#">access.re</a>  |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC    | <a href="#">access.re</a>  |
| [SECURITY] [DLA 2970-1] qemu security update   | MLIST   | <a href="#">lists.debi</a> |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC    | <a href="#">access.re</a>  |
| CVE-2021-20196 QEMU Vulnerability in NetApp Products   NetApp Product Security                               | CONFIRM | <a href="#">security.r</a> |
| oss-security - CVE-2021-20196 QEMU: block: fdc: null pointer dereference may lead to guest crash             | MISC    | <a href="#">www.ope</a>    |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC    | <a href="#">access.re</a>  |
| CVE Program record   | CVE.ORG | <a href="#">www.cve</a>    |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

|   |
|---|
| <a href="#">159638</a> Oracle Enterprise Linux Security Update for qemu (ELSA-2022-9123)                      |
| <a href="#">159672</a> Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2022-9172)                 |
| <a href="#">159858</a> Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2022-1759) |
| <a href="#">179172</a> Debian Security Update for qemu (DLA 2970-1)   |
| <a href="#">180995</a> Debian Security Update for qemu (DLA 3099-1)   |
| <a href="#">182006</a> Debian Security Update for qemu (CVE-2021-20196)                                       |
| <a href="#">198683</a> Ubuntu Security Notification for QEMU Vulnerabilities (USN-5307-1)                     |
| <a href="#">240292</a> Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2022:1759)             |
| <a href="#">355320</a> Amazon Linux Security Advisory for qemu : ALAS2-2023-2061                              |
| <a href="#">502168</a> Alpine Linux Security Update for qemu  |
| <a href="#">751661</a> OpenSUSE Security Update for qemu (openSUSE-SU-2022:0177-1)                            |
| <a href="#">751671</a> OpenSUSE Security Update for qemu (openSUSE-SU-2022:0210-1)                            |
| <a href="#">751742</a> OpenSUSE Security Update for qemu (openSUSE-SU-2022:0210-2)                            |
| <a href="#">751985</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:0177-1)                   |
| <a href="#">752033</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:1151-1)                   |
| <a href="#">940525</a> AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2022:1759)           |
| <a href="#">960314</a> Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2022:1759)         |

© [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](#)**