



CVE-2021-3507

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

Summary

| | |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2021-3507 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-05-06 16:15:00 UTC |
| Updated | 2023-02-12 23:41:00 UTC |
| Description | A heap buffer overflow was found in the floppy disk emulator of QEMU up to 6.0.0 (including). It could occur in fdctrl_transf |

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |

References

| Reference | Source | Link |
|----------------------------------------------------------------------------------------------------|---------|-------------------------------------|
| CVE-2021-3507 QEMU Vulnerability in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com |
| [SECURITY] [DLA 3099-1] qemu security update | MLIST | lists.debian.org |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | MISC | access.redhat.com |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | MISC | access.redhat.com |
| 1951118 – (CVE-2021-3507) CVE-2021-3507 QEMU: fdc: heap buffer overflow in DMA read data transfers | MISC | bugzilla.redhat.com |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | MISC | access.redhat.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|-----------------------------------------------------------------------------------------------|
| 160006 Oracle Enterprise Linux Security Update for qemu (ELSA-2022-9669) |
| 160027 Oracle Enterprise Linux Security Update for virt:kvm_utils (ELSA-2022-9700) |
| 160248 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2022-7472) |
| 160273 Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-2022-7967) |
| 180995 Debian Security Update for qemu (DLA 3099-1) |
| 182040 Debian Security Update for qemu (CVE-2021-3507) |
| 198837 Ubuntu Security Notification for QEMU Vulnerabilities (USN-5489-1) |
| 240837 Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2022:7472) |
| 240913 Red Hat Update for qemu-kvm security (RHSA-2022:7967) |
| 502356 Alpine Linux Security Update for qemu |
| 752725 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3768-1) |
| 753802 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0761-1) |
| 753824 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0840-1) |
| 753840 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0878-1) |
| 900063 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0 |
| 903359 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (4186) |
| 940832 AlmaLinux Security Update for qemu-kvm (ALSA-2022:7967) |
| 960170 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2022:7472) |
| 960500 Rocky Linux Security Update for qemu-kvm (RLSA-2022:7967) |

© [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](#)