



CVE-2021-3750

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

Summary

CVE	CVE-2021-3750
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-02 19:15:00 UTC
Updated	2023-02-12 23:42:00 UTC
Description	A DMA reentrancy issue was found in the USB EHCI controller emulation of QEMU. EHCI does not verify if the Buffer Point

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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-2021-3750 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
Fix DMA MMIO reentrancy issues (#556) · Issues · QEMU / QEMU · GitLab	MISC	gitlab.com
1999073 – (CVE-2021-3750) CVE-2021-3750 QEMU: hcd-ehci: DMA reentrancy issue leads to use-after-free	MISC	bugzilla.redhat.com
Heap-use-after-free through ehci_flush_qh (#541) · Issues · QEMU / QEMU · GitLab	MISC	gitlab.com
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	security.gentoo.org
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

160273	Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-2022-7967)
161176	Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2023-6980)
161478	Oracle Enterprise Linux Security Update for virt:kvm_utils3 (ELSA-2024-12276)
183308	Debian Security Update for qemu (CVE-2021-3750)
199069	Ubuntu Security Notification for QEMU Vulnerabilities (USN-5772-1)
240913	Red Hat Update for qemu-kvm security (RHSA-2022:7967)
242430	Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2023:6980)
242778	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2024:0569)
242861	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2024:0404)
379624	Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2024:0021)
710604	Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
754898	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3721-1)
754937	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3800-1)
755084	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:4056-1)
901579	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9707)
901933	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9701)
902503	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9707-1)
907029	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9701-1)
940832	AlmaLinux Security Update for qemu-kvm (ALSA-2022:7967)
941431	AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2023:6980)
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](#)