



CVE-2021-4145

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

Summary

CVE	CVE-2021-4145
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-25 20:15:00 UTC
Updated	2022-09-28 19:54:00 UTC
Description	A NULL pointer dereference issue was found in the block mirror layer of QEMU in versions prior to 6.2.0. The `self` pointer

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	6.1.0	-	All	All
Application	Qemu	Qemu	6.1.0	rc0	All	All
Application	Qemu	Qemu	6.1.0	rc1	All	All
Application	Qemu	Qemu	6.1.0	rc2	All	All
Application	Qemu	Qemu	6.1.0	rc3	All	All
Application	Qemu	Qemu	6.1.0	rc4	All	All
Application	Qemu	Qemu	6.2.0	rc0	All	All
Application	Qemu	Qemu	6.2.0	rc1	All	All
Application	Qemu	Qemu	6.2.0	rc2	All	All
Application	Qemu	Qemu	6.2.0	rc3	All	All
Application	Qemu	Qemu	6.2.0	rc4	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source
block/mirror: fix NULL pointer dereference in mirror_wait_on_conflicts() (66fed30c) · Commits · QEMU / QEMU · GitLab	MISC

CVE-2021-4145 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO
2034602 – (CVE-2021-4145) CVE-2021-4145 QEMU: NULL pointer dereference in mirror_wait_on_conflicts() in block/mirror.c	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159771 Oracle Enterprise Linux Security Update for qemu (ELSA-2022-9344)
159792 Oracle Enterprise Linux Security Update for virt:kvm_utils (ELSA-2022-9364)
159858 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2022-1759)
182495 Debian Security Update for qemu (CVE-2021-4145)
240292 Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2022:1759)
710604 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
900621 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (8346)
900982 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (8347)
902115 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (8347-1)
940525 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2022:1759)
960314 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](#)