



CVE-2022-0358

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

Summary

CVE	CVE-2022-0358
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-29 15:15:00 UTC
Updated	2022-12-09 18:00:00 UTC
Description	A flaw was found in the QEMU virtio-fs shared file system daemon (virtiofsd) implementation. This flaw is strictly related to C

Risk And Classification

Problem Types: CWE-273

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

References

Reference	Source	Lir
CVE-2022-0358 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM	sec
virtiofsd: Drop membership of all supplementary groups (CVE-2022-0358) (449e8171) · Commits · QEMU / QEMU · GitLab	MISC	gitl
2044863 – (CVE-2022-0358) CVE-2022-0358 QEMU: virtiofsd: potential privilege escalation via CVE-2018-13405	MISC	bu
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	acc
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159713](#) Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2022-0886)

[179273](#) Debian Security Update for qemu (DSA 5133-1)

184085 Debian Security Update for qemu (CVE-2022-0358)
198683 Ubuntu Security Notification for QEMU Vulnerabilities (USN-5307-1)
198837 Ubuntu Security Notification for QEMU Vulnerabilities (USN-5489-1)
240119 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2022:0759)
240150 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2022:0886)
282383 Fedora Security Update for qemu (FEDORA-2022-3a60c34473)
282444 Fedora Security Update for qemu (FEDORA-2022-5d0676b098)
354314 Amazon Linux Security Advisory for qemu : ALAS2022-2022-050
377397 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0022)
710604 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
751920 OpenSUSE Security Update for qemu (openSUSE-SU-2022:0930-1)
752009 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:0930-1)
903829 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (10763-1)
904795 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (10782)
905193 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (10782-1)
905889 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (10782-2)
940472 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2022:0886)
960800 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2022:0886)

© [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](#)