



CVE-2021-3975

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

Summary

CVE	CVE-2021-3975
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-23 20:15:00 UTC
Updated	2024-04-01 13:16:00 UTC
Description	A use-after-free flaw was found in libvirt. The qemuMonitorUnregister() function in qemuProcessHandleMonitorEOF is calle

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	Canonical	Ubuntu Linux	21.10	All
Operating System	Debian	Debian Linux	10.0	All
Operating System	Debian	Debian Linux	11.0	All
Operating System	Fedoraproject	Fedora	35	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All
Application	Redhat	Codeready Linux Builder	-	All
Operating System	Redhat	Enterprise Linux	8.0	All
Operating System	Redhat	Enterprise Linux	8.0	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.6	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.6	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.6	All

Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.6	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	8.6	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All
Application	Redhat	Libvirt	All	All

References

Reference	Source	Link
CVE-2021-3975 Ubuntu	MISC	ubuntu.co
[debian-lts-announce] 20240401 [SECURITY] [DLA 3778-1] libvirt security update		lists.debian
qemu: Add missing lock in qemuProcessHandleMonitorEOF · libvirt/libvirt@1ac703a · GitHub	MISC	github.com
2024326 – (CVE-2021-3975) CVE-2021-3975 libvirt: segmentation fault during VM shutdown can lead to vdsmd hang	MISC	bugzilla.redhat.com
CVE-2021-3975 Libvirt 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
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

159858 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2022-1759)
160002 Oracle Enterprise Linux Security Update for libvirt libvirt-python (ELSA-2022-9668)
160027 Oracle Enterprise Linux Security Update for virt:kvm_utils (ELSA-2022-9700)
182886 Debian Security Update for libvirt (CVE-2021-3975)
198763 Ubuntu Security Notification for libvirt Vulnerabilities (USN-5399-1)
240292 Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2022:1759)
6000552 Debian Security Update for libvirt (DLA 3778-1)
751580 SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2022:0031-1)
751581 SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2022:0032-1)
751585 SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2022:0041-1)
751586 SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2022:0042-1)
751588 SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2022:0045-1)
751620 SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2022:0128-1)

903768 Common Base Linux Mariner (CBL-Mariner) Security Update for libvirt (10645)

904201 Common Base Linux Mariner (CBL-Mariner) Security Update for libvirt (10645-1)

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](#)