



CVE-2020-25637

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

Summary

CVE	CVE-2020-25637
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-06 14:15:00 UTC
Updated	2024-04-01 13:16:00 UTC
Description	A double free memory issue was found to occur in the libvirt API, in versions before 6.8.0, responsible for requesting inform

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Libvirt	All	All	All	All
Application	Redhat	Libvirt	All	All	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2020:1777-1: important: Security update	SUSE	lists.opensu
[debian-lts-announce] 20240401 [SECURITY] [DLA 3778-1] libvirt security update		lists.debian.
libvirt: Multiple Vulnerabilities (GLSA 202210-06) — Gentoo security	GENTOO	security.ger
1881037 – (CVE-2020-25637) CVE-2020-25637 libvirt: double free in qemuAgentGetInterfaces() in qemu_agent.c	MISC	bugzilla.red

[security-announce] openSUSE-SU-2020:1778-1: important: Security update	SUSE	lists.opensuse.org
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

[159456](#) Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-1762)

[198763](#) Ubuntu Security Notification for libvirt Vulnerabilities (USN-5399-1)

[239306](#) Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:1762)

[377413](#) Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)

[377483](#) Alibaba Cloud Linux Security Update for libvirt (ALINUX2-SA-2020:0182)

[500327](#) Alpine Linux Security Update for libvirt

[501613](#) Alpine Linux Security Update for libvirt

[6000552](#) Debian Security Update for libvirt (DLA 3778-1)

[710643](#) Gentoo Linux libvirt Multiple Vulnerabilities (GLSA 202210-06)

[900185](#) CBL-Mariner Linux Security Update for libvirt 6.1.0

[901534](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libvirt (6658-1)

[903345](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libvirt (3113)

[940118](#) AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:1762)

[960265](#) Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:1762)

© [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](#)