



CVE-2021-3667

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-3667
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-02 23:15:00 UTC
Updated	2024-04-01 13:16:00 UTC
Description	An improper locking issue was found in the virStoragePoolLookupByTargetPath API of libvirt. It occurs in the storagePoolLc

Risk And Classification

Problem Types: CWE-667

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Libvirt	All	All	All	All

References

Reference	Source
libvirt.org Git - libvirt.git/commit	MISC
lists.debian.org/debian-lts-announce/2024/04/msg00000.html	
1986094 – (CVE-2021-3667) CVE-2021-3667 libvirt: Improper locking on ACL failure in virStoragePoolLookupByTargetPath API	MISC
storage_driver: Unlock object on ACL fail in storagePoolLookupByTargetPath (447f69de) · Commits · libvirt / libvirt · GitLab	MISC
CVE-2021-3667 Libvirt Vulnerability in NetApp Products NetApp Product Security	CONFIRM
libvirt: Multiple Vulnerabilities (GLSA 202210-06) — Gentoo security	GENTOO
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
libvirt.org Git	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159468](#) Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2021-4191)

[183057](#) Debian Security Update for libvirt (CVE-2021-3667)

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

[239833](#) Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2021:4191)

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

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

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

[751003](#) OpenSUSE Security Update for libvirt (openSUSE-SU-2021:2812-1)

[751189](#) SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2021:3277-1)

[751282](#) SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2021:3540-1)

[751327](#) OpenSUSE Security Update for libvirt (openSUSE-SU-2021:1451-1)

[900734](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libvirt (8881)

[940172](#) AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:4191)

[960274](#) Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:4191)

© [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](#)