



CVE-2021-3559

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

Summary

CVE	CVE-2021-3559
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-24 12:15:00 UTC
Updated	2022-04-26 16:25:00 UTC
Description	A flaw was found in libvirt in the virConnectListAllNodeDevices API in versions before 7.0.0. It only affects hosts with a PCI

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Redhat	Libvirt	All	All	All	All
Application	Redhat	Libvirt	7.0.0	rc1	All	All
Application	Redhat	Libvirt	7.0.0	rc2	All	All

References

Reference	Source
1962306 – (CVE-2021-3559) CVE-2021-3559 libvirt: nodedev-list command may cause libvirt to crash on hosts with GRID driver installed	M
CVE-2021-3559 Libvirt Vulnerability in NetApp Products NetApp Product Security	C
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[900035](#) CBL-Mariner Linux Security Update for libvirt 6.1.0

© [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](#)