



CVE-2021-3947

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

Summary

CVE	CVE-2021-3947
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-18 18:15:00 UTC
Updated	2023-11-21 21:38:00 UTC
Description	A stack-buffer-overflow was found in QEMU in the NVME component. The flaw lies in nvme_changed_nslist() where a mali

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	6.2.0	-	All	All
Application	Qemu	Qemu	6.2.0	rc0	All	All
Application	Qemu	Qemu	6.2.0	rc1	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2021-3947 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
2021869 – (CVE-2021-3947) CVE-2021-3947 QEMU: NVME: Arbitrary Memory Read	MISC	bugzilla.redhat.com	
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159638 Oracle Enterprise Linux Security Update for qemu (ELSA-2022-9123)
159672 Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2022-9172)
183954 Debian Security Update for qemu (CVE-2021-3947)
502168 Alpine Linux Security Update for qemu
710604 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
900709 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (8688)
901146 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (8672)
902083 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (8672-1)
906027 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (8688-1)

© [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](#)