



# CVE-2021-3929

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

## Summary

<b>CVE</b>	CVE-2021-3929
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-25 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:38:00 UTC
<b>Description</b>	A DMA reentrancy issue was found in the NVM Express Controller (NVME) emulation in QEMU. This CVE is similar to CVE

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	7.0.0	-	All	All

## References

Reference	Source	Link
2020298 – (CVE-2021-3929) CVE-2021-3929 QEMU: nvme: DMA reentrancy issue leads to use-after-free	MISC	<a href="#">bugzilla.redha</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.redhat</a>
nvme: DMA reentrancy issue leads to use-after-free (CVE-2021-3929) (#782) · Issues · QEMU / QEMU · GitLab	MISC	<a href="#">gitlab.com</a>
hw/nvme: fix CVE-2021-3929 (736b0164) · Commits · QEMU / QEMU · GitLab	MISC	<a href="#">gitlab.com</a>
Fix DMA MMIO reentrancy issues (#556) · Issues · QEMU / QEMU · GitLab	MISC	<a href="#">gitlab.com</a>
[SECURITY] Fedora 36 Update: qemu-6.2.0-15.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorapro</a>
[SECURITY] Fedora 36 Update: qemu-6.2.0-15.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedorapro</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

182950	Debian Security Update for qemu (CVE-2021-3929)
198837	Ubuntu Security Notification for QEMU Vulnerabilities (USN-5489-1)
283141	Fedora Security Update for qemu (FEDORA-2022-f0a2695054)
710604	Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
753802	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0761-1)
753824	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0840-1)
754898	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3721-1)
754937	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3800-1)
903787	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (10725)
903830	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (10721)
905240	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (10721-1)

© [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](#)