



CVE-2021-3607

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

Summary

CVE	CVE-2021-3607
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-24 19:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	An integer overflow was found in the QEMU implementation of VMWare's paravirtual RDMA device in versions prior to 6.1.0

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source
[SECURITY] [DLA 3099-1] qemu security update	MLIST
1973349 – (CVE-2021-3607) CVE-2021-3607 QEMU: pvrmda: unchecked malloc size due to integer overflow in init_dev_ring()	MISC
[PATCH] pvrmda: Ensure correct input on ring init (CVE-2021-3607)	MISC
February 2022 QEMU Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159368 Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9425)
159465 Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9425)
159566 Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2021-9568)
180201 Debian Security Update for qemu (CVE-2021-3607)
180995 Debian Security Update for qemu (DLA 3099-1)
198432 Ubuntu Security Notification for QEMU vulnerabilities (USN-5010-1)
710604 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
750874 OpenSUSE Security Update for qemu (openSUSE-SU-2021:2442-1)
750879 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:2448-1)
750901 OpenSUSE Security Update for qemu (openSUSE-SU-2021:2474-1)
750910 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:2591-1)
750912 OpenSUSE Security Update for qemu (openSUSE-SU-2021:2591-1)
751053 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1202-1)
900705 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (8814)

© [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](#)