



CVE-2021-20221

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

Summary

CVE	CVE-2021-20221
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-13 16:15:00 UTC
Updated	2023-11-07 03:29:00 UTC
Description	An out-of-bounds heap buffer access issue was found in the ARM Generic Interrupt Controller emulator of QEMU up to and

Risk And Classification

Problem Types: CWE-125

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	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
1924601 – (CVE-2021-20221) CVE-2021-20221 qemu: out-of-bound heap buffer access via an interrupt ID field	MISC	bugzilla.redha
oss-security - CVE-2021-20221 QEMU: aarch64: GIC: out-of-bound heap buffer access via an interrupt ID field	MISC	www.openwal
CVE-2021-20221 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netap
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat
Bug #1914353 "QEMU: aarch64: :GIC: out-of-bounds access via inte...": Bugs : QEMU	MISC	bugs.launchp
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.debian.or
[SECURITY] [DLA 2560-1] qemu security update	MLIST	lists.debian.or
oss-security - CVE-2021-20221 QEMU: aarch64: GIC: out-of-bound heap buffer access via an interrupt ID field	MLIST	www.openwal

Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159250 Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9285)
159343 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-3061)
159566 Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2021-9568)
174921 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)
174923 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)
174924 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)
174926 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1242-1)
180227 Debian Security Update for qemu (CVE-2021-20221)
180995 Debian Security Update for qemu (DLA 3099-1)
198432 Ubuntu Security Notification for QEMU vulnerabilities (USN-5010-1)
239539 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061)
377346 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2021:0058)
502351 Alpine Linux Security Update for qemu
671198 EulerOS Security Update for qemu (EulerOS-SA-2022-1034)
671203 EulerOS Security Update for qemu (EulerOS-SA-2022-1014)
750124 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1894-1)
750338 OpenSUSE Security Update for qemu (openSUSE-SU-2021:0363-1)
900156 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
903375 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (4272)
940064 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:3061)
960072 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:3061)

© [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](#)