



CVE-2021-4207

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

Summary

CVE	CVE-2021-4207
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-29 17:15:00 UTC
Updated	2023-11-07 03:40:00 UTC
Description	A flaw was found in the QXL display device emulation in QEMU. A double fetch of guest controlled values `cursor->header.

Risk And Classification

Problem Types: CWE-362 | CWE-120

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	11.0	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
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.c
Debian -- Security Information -- DSA-5133-1 qemu	DEBIAN	www.
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	secu
2036966 – (CVE-2021-4207) CVE-2021-4207 QEMU: QXL: double fetch in qxl_cursor() can lead to heap buffer overflow	MISC	bugzi
STAR Labs Advisories QEMU QXL Integer overflow leads to Heap Overflow	MISC	starla
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160006 Oracle Enterprise Linux Security Update for qemu (ELSA-2022-9669)
160024 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2022-5821)
160027 Oracle Enterprise Linux Security Update for virt:kvm_utils (ELSA-2022-9700)
160134 Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-2022-9869)
160141 Oracle Enterprise Linux Security Update for kvm_utils2 (ELSA-2022-9862)
179273 Debian Security Update for qemu (DSA 5133-1)
180995 Debian Security Update for qemu (DLA 3099-1)
183560 Debian Security Update for qemu (CVE-2021-4207)
198837 Ubuntu Security Notification for QEMU Vulnerabilities (USN-5489-1)
240585 Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2022:5821)
355320 Amazon Linux Security Advisory for qemu : ALAS2-2023-2061
377638 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0168)
710604 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
752284 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:2254-1)
752288 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:2260-1)
752675 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3594-1)
752725 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3768-1)
754224 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3015-1)
901297 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9626)
901451 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9619)
905184 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9626-1)
905243 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9619-1)
940607 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2022:5821)
960299 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2022:5821)

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](#)