CVE-2021-4206

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-4206
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. An integer overflow in the cursor_alloc() function can lead

Risk And Classification

Problem Types: CWE-190 | CWE-120 | CWE-131

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
2036998 – (CVE-2021-4206) CVE-2021-4206 QEMU: QXL: integer overflow in cursor_alloc() can lead to heap buffer overflow	MISC
[SECURITY] [DLA 3099-1] qemu security update	MLIST
Debian -- Security Information -- DSA-5133-1 qemu	DEBIAN
STAR Labs | Advisories | QEMU QXL Integer overflow leads to Heap Overflow	MISC
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

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)

184245 Debian Security Update for qemu (CVE-2021-4206)

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)

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)

753802 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0761-1)

901290 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9625)

901661 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9618)

902306 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9618-1)

902505 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9625-1)

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)

© 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 registred 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