CVE-2022-4144

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-4144
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-29 18:15:00 UTC
Updated	2023-11-07 03:57:00 UTC
Description	An out-of-bounds read flaw was found in the QXL display device emulation in QEMU. The qxl_phys2virt() function does not

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	Extra Packages For Enterprise Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Sourc
CVE-2022-4144 QEMU Vulnerability in NetApp Products | NetApp Product Security	CONF
[SECURITY] Fedora 36 Update: qemu-6.2.0-17.fc36 - package-announce - Fedora Mailing-Lists	
[RFC PATCH-for-7.2 4/4] hw/display/qxl: Avoid buffer overrun in qxl_phys	MISC
[SECURITY] Fedora 36 Update: qemu-6.2.0-17.fc36 - package-announce - Fedora Mailing-Lists	FEDO
[SECURITY] Fedora 37 Update: qemu-7.0.0-12.fc37 - package-announce - Fedora Mailing-Lists	FEDO
2148506 – (CVE-2022-4144) CVE-2022-4144 QEMU: QXL: qxl_phys2virt unsafe address translation can lead to out-of-bounds read	MISC
[SECURITY] Fedora 37 Update: qemu-7.0.0-12.fc37 - package-announce - Fedora Mailing-Lists	
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160395 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2023-0099)

160507 Oracle Enterprise Linux Security Update for virt:kvm_utils2 (ELSA-2023-12195)

160606 Oracle Enterprise Linux Security Update for virt:kvm_utils (ELSA-2023-12342)

160711 Oracle Enterprise Linux Security Update for qemu (ELSA-2023-12368)

184144 Debian Security Update for qemu (CVE-2022-4144)

199428 Ubuntu Security Notification for QEMU Vulnerabilities (USN-6167-1)

241052 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2023:0099)

241131 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2023:0432)

283510 Fedora Security Update for qemu (FEDORA-2022-22b1f8dae2)

283617 Fedora Security Update for qemu (FEDORA-2023-c8a60f6f80)

355320 Amazon Linux Security Advisory for qemu : ALAS2-2023-2061

377995 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2023:0019)

672787 EulerOS Security Update for kata-containers (EulerOS-SA-2023-1564)

672799 EulerOS Security Update for kata-containers (EulerOS-SA-2023-1539)

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)

753840 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0878-1)

753841 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0877-1)

904589 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (11570)

904592 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (11522)

904774 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (11522-1)

940869 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2023:0099)

960533 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2023:0099)

CVE.report and Source URL Uptime Status status.cve.report