CVE-2023-3354

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-3354
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-11 17:15:00 UTC
Updated	2024-03-11 18:15:00 UTC
Description	A flaw was found in the QEMU built-in VNC server. When a client connects to the VNC server, QEMU checks whether the c

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	-	All	All	All
Application	Qemu	Qemu	8.1.0	rc0	All	All
Application	Qemu	Qemu	8.1.0	rc1	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All

References

Reference
lists.debian.org/debian-lts-announce/2024/03/msg00012.html
cve-details
2216478 – (CVE-2023-3354) CVE-2023-3354 QEMU: VNC: improper I/O watch removal in TLS handshake can lead to remote unauthenticate
[SECURITY] Fedora 38 Update: qemu-7.2.5-1.fc38 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160935 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2023-5264)

160960 Oracle Enterprise Linux Security Update for kvm_utils3 (ELSA-2023-12855)

242071 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2023:5264)

242077 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2023:5239)

242144 Red Hat Update for virt:rhel (RHSA-2023:5587)

242190 Red Hat Update for virt:rhel (RHSA-2023:5796)

242262 Red Hat Update for qemu-kvm (RHSA-2023:6227)

242861 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2024:0404)

378927 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2023:0125)

6000518 Debian Security Update for qemu (DLA 3759-1)

673490 EulerOS Security Update for qemu (EulerOS-SA-2023-2887)

673611 EulerOS Security Update for qemu-micro (EulerOS-SA-2023-3193)

673823 EulerOS Security Update for qemu (EulerOS-SA-2023-3153)

673919 EulerOS Security Update for qemu (EulerOS-SA-2023-2906)

674008 EulerOS Security Update for qemu-micro (EulerOS-SA-2023-3228)

754898 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3721-1)

754937 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3800-1)

755084 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:4056-1)

755451 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:4662-1)

755817 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2024:0589-1)

907663 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (31659)

907673 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (31659-1)

941250 AlmaLinux Security Update for qemu-kvm (ALSA-2023:5094)

941271 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2023:5264)