CVE-2009-3616

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-3616
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-23 18:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Multiple use-after-free vulnerabilities in vnc.c in the VNC server in QEMU 0.10.6 and earlier might allow guest OS users to e

Risk And Classification

Primary CVSS: v3.1 9.9 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Problem Types: CWE-416 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	8.5		AV:N/AC:M/Au:S/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
qemu.git -	af854a3a-2
508567 – Virtual Machine aborts abrupt when executing rdesktop localhost:5900 command	af854a3a-2
oss-security - Re: QEMU VNC use-after-free	af854a3a-2
QEMU VNC Client Disconnect Use After Free Remote Code Execution Vulnerability	af854a3a-2
oss-security - QEMU VNC use-after-free	af854a3a-2
501131 – qemu segfault when VNC client disconnects	af854a3a-2
'Re: [Qemu-devel] [STABLE] [BUG] VNC mode can crash QEMU' - MARC	af854a3a-2
qemu.git -	af854a3a-2

Red Hat Customer Portal	af854a3a-2
505641 – (CVE-2009-3616) CVE-2009-3616 Remote VNC client can cause any QEMU VNC server to crash with a double-free	af854a3a-2
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.