# CVE Detail – CVE-2009-3616

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 execute arbitrary code on the host OS by establishing a connection from a VNC client and then (1) disconnecting during data transfer, (2) sending a message using incorrect integer data types, or (3) using the Fuzzy Screen Mode protocol, related to double free vulnerabilities.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.74049

## CVSS Scoring

CVSS v3.1 Score: 9.9

Severity: CRITICAL

## Mapped CWE(s)

* CWE-416: Use After Free

## Affected Products

* cpe:2.3:a:qemu:qemu:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:5.0:\*:\*:\*:\*:\*:\*:\*