CVE-2015-5279

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

Summary

CVE	CVE-2015-5279
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-28 16:59:00 UTC
Updated	2023-02-13 00:52:00 UTC
Description	Heap-based buffer overflow in the ne2000_receive function in hw/net/ne2000.c in QEMU before 2.4.0.1 allows guest OS us

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All

References

Reference
git.qemu.org Git - qemu.git/commit
[SECURITY] Fedora 22 Update: qemu-2.3.1-5.fc22
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
[security-announce] SUSE-SU-2015:1782-1: important: Security update for
[SECURITY] Fedora 23 Update: qemu-2.4.0-4.fc23
Debian -- Security Information -- DSA-3362-1 qemu-kvm
oss-security - CVE-2015-5279 Qemu: net: add checks to validate ring buffer pointers
QEMU Buffer Overflow in ne2000_receive() Lets Local Guest Users Deny Service or Execute Arbitrary Code on the Host System - SecurityTra
Red Hat Customer Portal
Bug 1256672 – CVE-2015-5279 qemu: Heap overflow vulnerability in ne2000_receive() function
Red Hat Customer Portal

Red Hat Customer Portal
git.qemu.org Git - qemu.git/commit
Arista - Security Advisory 0014
[SECURITY] Fedora 21 Update: qemu-2.1.3-11.fc21
Oracle Linux Bulletin - October 2015
Red Hat Customer Portal
Red Hat Customer Portal
CVE-2015-5279 - Red Hat Customer Portal
Debian -- Security Information -- DSA-3361-1 qemu
QEMU NE2000 NIC Emulation Heap Based Buffer Overflow Vulnerability
Red Hat Customer Portal
[Qemu-devel] [PULL 2/3] net: add checks to validate ring buffer pointers
QEMU: Multiple vulnerabilities (GLSA 201602-01) — Gentoo security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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