CVE-2015-8744

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-8744
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-29 22:59:00 UTC
Updated	2023-02-13 00:55:00 UTC
Description	QEMU (aka Quick Emulator) built with a VMWARE VMXNET3 paravirtual NIC emulator support is vulnerable to crash issue

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference
Debian -- Security Information -- DSA-3471-1 qemu
oss-security - CVE request Qemu: net: vmxnet3: incorrect l2 header validation leads to a crash
QEMU 'net/vmxnet3.c' Denial of Service Vulnerability
git.qemu.org Git - qemu.git/commitdiff
QEMU VMXNET3 Packet Processing Error Lets Local Users on a Guest System Cause Denial of Service Conditions on the Host System - Se
oss-security - Re: CVE request Qemu: net: vmxnet3: incorrect l2 header validation leads to a crash
git.qemu.org Git - qemu.git/commitdiff
Bug 1270871 – CVE-2015-8744 Qemu: net: vmxnet3: incorrect l2 header validation leads to a crash via assert(2) call
QEMU: Multiple vulnerabilities (GLSA 201602-01) — Gentoo security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

900063 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0