



# CVE-2015-8744

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2015-8744
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-12-29 22:59:00 UTC
<b>Updated</b>	2023-02-13 00:55:00 UTC
<b>Description</b>	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	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All

## References

### Reference

<a href="#">Debian -- Security Information -- DSA-3471-1 qemu</a>
<a href="#">oss-security - CVE request Qemu: net: vmxnet3: incorrect I2 header validation leads to a crash</a>
<a href="#">QEMU 'net/vmxnet3.c' Denial of Service Vulnerability</a>
<a href="#">git.qemu.org Git - qemu.git/commitdiff</a>
<a href="#">QEMU VMXNET3 Packet Processing Error Lets Local Users on a Guest System Cause Denial of Service Conditions on the Host System - Se</a>
<a href="#">oss-security - Re: CVE request Qemu: net: vmxnet3: incorrect I2 header validation leads to a crash</a>
<a href="#">git.qemu.org Git - qemu.git/commitdiff</a>
<a href="#">Bug 1270871 – CVE-2015-8744 Qemu: net: vmxnet3: incorrect I2 header validation leads to a crash via assert(2) call</a>
<a href="#">QEMU: Multiple vulnerabilities (GLSA 201602-01) — Gentoo security</a>
<a href="#">CVE Program record</a>
<a href="#">NVD vulnerability detail</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[900063](#) CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)