



CVE-2016-1981

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

Summary

CVE	CVE-2016-1981
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-29 22:59:00 UTC
Updated	2023-02-12 23:17:00 UTC
Description	QEMU (aka Quick Emulator) built with the e1000 NIC emulation support is vulnerable to an infinite loop issue. It could occur

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-3471-1 qemu	DEBIAN	www.debian.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
oss-security - Re: CVE request Qemu: net: e1000 infinite loop in start_xmit and e1000_receive_iov routines	MLIST	www.openwall.co
Debian -- Security Information -- DSA-3469-1 qemu	DEBIAN	www.debian.org
CVE-2016-1981 - Red Hat Customer Portal	MISC	access.redhat.co
Debian -- Security Information -- DSA-3470-1 qemu-kvm	DEBIAN	www.debian.org
Red Hat Customer Portal	MISC	access.redhat.co
Bug 1298570 – CVE-2016-1981 Qemu: net: e1000 infinite loop in start_xmit and e1000_receive_iov routines	CONFIRM	bugzilla.redhat.co
oss-security - CVE request Qemu: net: e1000 infinite loop in start_xmit and e1000_receive_iov routines	MLIST	www.openwall.co

QEMU CVE-2016-1981 Multiple Denial of Service Vulnerabilities	BID	www.securityfocus.com/bid/77100
QEMU: Multiple vulnerabilities (GLSA 201604-01) — Gentoo Security	GENTOO	security.gentoo.org/glsa/201604-01
[Qemu-devel] [PATCH] e1000: eliminate infinite loops on out-of-bounds tr	MLIST	lists.gnu.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)