



# CVE-2018-17963

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

## Summary

<b>CVE</b>	CVE-2018-17963
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-10-09 22:29:00 UTC
<b>Updated</b>	2021-08-04 17:14:00 UTC
<b>Description</b>	qemu_deliver_packet_iov in net/net.c in Qemu accepts packet sizes greater than INT_MAX, which allows attackers to caus

## Risk And Classification

### Problem Types: CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
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>	9.0	All	All	All
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>	9.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	rc0	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	rc1	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	rc2	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	rc3	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	rc0	All	All

Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	rc1	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	rc2	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	rc3	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	10	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	13	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	13.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	14	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	10	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	13.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	14	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization Manager</a>	4.3	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization Manager</a>	4.3	All	All	All

## References

Reference	Source	Link	Tags
[Qemu-devel] [PATCH for 3.1 0/4] Fix possible OOB during queuing packets	MISC	<a href="https://lists.gnu.org">lists.gnu.org</a>	Mailing List, Patch, Third Pa
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
[SECURITY] [DLA 1599-1] qemu security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing List, Third Party Adv
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
oss-security - Qemu: integer overflow issues	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, Third Party Adv
[Qemu-devel] [PULL 24/25] net: ignore packet size greater than INT_MAX	MLIST	<a href="https://lists.gnu.org">lists.gnu.org</a>	Mailing List, Patch, Third Pa
USN-3826-1: QEMU vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Debian -- Security Information -- DSA-4338-1 qemu	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[377259](#) Alibaba Cloud Linux Security Update for qemu-kvm-ma (ALINUX2-SA-2020:0007)

© [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](#)**