



# CVE-2020-28916

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

## Summary

<b>CVE</b>	CVE-2020-28916
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-04 07:15:00 UTC
<b>Updated</b>	2022-09-30 19:19:00 UTC
<b>Description</b>	hw/net/e1000e_core.c in QEMU 5.0.0 has an infinite loop via an RX descriptor with a NULL buffer address.

## Risk And Classification

**Problem Types:** CWE-835

## 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>	10.0	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>	9.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	5.0.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	5.0.0	All	All	All

## References

Reference	Source	Link	Ta
Re: [PATCH] hw/net/e1000e: advance desc_offset in case of null descripto	MISC	<a href="https://lists.nongnu.org">lists.nongnu.org</a>	E:
[SECURITY] [DLA 3099-1] qemu security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
[SECURITY] [DLA 2560-1] qemu security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	M
oss-security - CVE-2020-28916 QEMU: e1000e: infinite loop scenario in case of null packet descriptor	CONFIRM	<a href="https://www.openwall.com">www.openwall.com</a>	M
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

## Legacy OID Mappings

159456 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-1762)
174920 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1243-1)
174921 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)
174922 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1240-1)
174923 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)
174924 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)
174926 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1242-1)
180995 Debian Security Update for qemu (DLA 3099-1)
239306 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:1762)
377413 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)
502352 Alpine Linux Security Update for qemu
750251 OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)
940118 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:1762)
960265 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:1762)

© [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](#)**