



# CVE-2020-15859

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

## Summary

<b>CVE</b>	CVE-2020-15859
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-07-21 16:15:00 UTC
<b>Updated</b>	2022-09-23 15:29:00 UTC
<b>Description</b>	QEMU 4.2.0 has a use-after-free in hw/net/e1000e_core.c because a guest OS user can trigger an e1000e packet with the

## Risk And Classification

**Problem Types:** CWE-416

## 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>	4.2.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	4.2.0	All	All	All

## References

Reference	Source	Link	Tags
oss-security - CVE-2020-15859 QEMU: net: e1000e: use-after-free while sending packets	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, P
[PATCH] e1000e: using bottom half to send packets	MISC	<a href="http://lists.gnu.org">lists.gnu.org</a>	Mailing List, P
[SECURITY] [DLA 3099-1] qemu security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	
[SECURITY] [DLA 2560-1] qemu security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing List, T
Bug #1886362 "Heap use-after-free in lduw_he_p through e1000e_wr..." : Bugs : QEMU	MISC	<a href="http://bugs.launchpad.net">bugs.launchpad.net</a>	Exploit, Issue
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, and

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159468](#) Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2021-4191)

[180995](#) Debian Security Update for qemu (DLA 3099-1)

[239833](#) Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2021:4191)

[377413](#) Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)

[502351](#) Alpine Linux Security Update for qemu

[710604](#) Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)

[900187](#) CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

[903486](#) Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1958)

[940172](#) AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:4191)

[960274](#) Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:4191)

© [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](#)