



# CVE-2021-20257

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

## Summary

<b>CVE</b>	CVE-2021-20257
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-16 15:15:00 UTC
<b>Updated</b>	2023-02-12 22:15:00 UTC
<b>Description</b>	An infinite loop flaw was found in the e1000 NIC emulator of the QEMU. This issue occurs while processing transmits (tx) d

## 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="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder</a>	-	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack Platform</a>	10.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack Platform</a>	13.0	All	All	All

## References

Reference	Source	Link
-----------	--------	------

Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.</a>
March 2022 QEMU Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security</a>
e1000: fail early for evil descriptor · qemu/qemu@3de46e6 · GitHub	MISC	<a href="#">github.c</a>
oss-security - CVE-2021-20257 QEMU: net: e1000: infinite loop while processing transmit descriptors	MISC	<a href="#">www.op</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.</a>
[SECURITY] [DLA 3099-1] qemu security update	MLIST	<a href="#">lists.dek</a>
1930087 – (CVE-2021-20257) CVE-2021-20257 QEMU: net: e1000: infinite loop while processing transmit descriptors	MISC	<a href="#">bugzilla</a>
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	<a href="#">security</a>
[PATCH] e1000: fail early for evil descriptor	MISC	<a href="#">lists.gnu</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.</a>
CVE Program record	CVE.ORG	<a href="#">www.cv</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">159294</a> Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9335)
<a href="#">159566</a> Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2021-9568)
<a href="#">159578</a> Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-5238)
<a href="#">159582</a> Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9638)
<a href="#">159672</a> Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2022-9172)
<a href="#">174875</a> SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:1023-1)
<a href="#">174920</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1243-1)
<a href="#">174921</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)
<a href="#">174922</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1240-1)
<a href="#">174923</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)
<a href="#">174924</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)
<a href="#">174926</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1242-1)
<a href="#">174928</a> SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:1252-1)
<a href="#">174929</a> SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:1251-1)
<a href="#">178540</a> Debian Security Update for qemu (DLA 2623-1)
<a href="#">179701</a> Debian Security Update for qemu (CVE-2021-20257)

180995	Debian Security Update for qemu (DLA 3099-1)
198432	Ubuntu Security Notification for QEMU vulnerabilities (USN-5010-1)
239978	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:5238)
355321	Amazon Linux Security Advisory for qemu : ALAS2-2023-2060
377413	Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)
502168	Alpine Linux Security Update for qemu
710604	Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
750097	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1837-1)
750120	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1893-1)
750124	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1894-1)
750129	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1895-1)
750138	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1918-1)
750152	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1947-1)
750251	OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)
750827	OpenSUSE Security Update for qemu (openSUSE-SU-2021:1043-1)
900764	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9056)
901546	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9068)
902039	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9056-1)
902098	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9068-1)
940065	AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:5238)
960270	Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:5238)

© 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](#)**