



# CVE-2021-3416

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-3416
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-18 20:15:00 UTC
<b>Updated</b>	2023-02-12 23:41:00 UTC
<b>Description</b>	A potential stack overflow via infinite loop issue was found in various NIC emulators of QEMU in versions up to and including

## 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="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	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>	7.0	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

## References

Reference	Source	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.re</a>
[SECURITY] [DLA 3099-1] qemu security update	MLIST	<a href="#">lists.debian</a>
[SECURITY] [DLA 2623-1] qemu security update	MLIST	<a href="#">lists.debian</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.re</a>
April 2021 QEMU Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.n</a>
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	<a href="#">security.g</a>

Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.re</a>
oss-security - CVE-2021-3416 QEMU: net: infinite loop in loopback mode may lead to stack overflow	MISC	<a href="#">www.oper</a>
1932827 – (CVE-2021-3416) CVE-2021-3416 QEMU: net: infinite loop in loopback mode may lead to stack overflow	MISC	<a href="#">bugzilla.re</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.o</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">159343</a> Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-3061)
<a href="#">159638</a> Oracle Enterprise Linux Security Update for qemu (ELSA-2022-9123)
<a href="#">159672</a> Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2022-9172)
<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="#">178540</a> Debian Security Update for qemu (DLA 2623-1)
<a href="#">179804</a> Debian Security Update for qemu (CVE-2021-3416)
<a href="#">180995</a> Debian Security Update for qemu (DLA 3099-1)
<a href="#">198432</a> Ubuntu Security Notification for QEMU vulnerabilities (USN-5010-1)
<a href="#">239539</a> Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061)
<a href="#">355614</a> Amazon Linux Security Advisory for qemu : ALAS2-2023-2148
<a href="#">377346</a> Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2021:0058)
<a href="#">502354</a> Alpine Linux Security Update for qemu
<a href="#">671198</a> EulerOS Security Update for qemu (EulerOS-SA-2022-1034)
<a href="#">671203</a> EulerOS Security Update for qemu (EulerOS-SA-2022-1014)
<a href="#">710604</a> Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
<a href="#">750149</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1942-1)

<a href="#">750251</a> OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)
<a href="#">750771</a> OpenSUSE Security Update for qemu (openSUSE-SU-2021:1942-1)
<a href="#">900218</a> CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
<a href="#">903645</a> Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (3996)
<a href="#">940064</a> AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:3061)
<a href="#">960072</a> Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:3061)

© [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](#)**