CVE-2021-3416

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

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

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

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

750251 OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)

750771 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1942-1)

900218 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

903645 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (3996)

940064 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:3061)

960072 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:3061)