



CVE-2021-20203

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

Summary

CVE	CVE-2021-20203
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-25 20:15:00 UTC
Updated	2022-09-30 19:32:00 UTC
Description	An integer overflow issue was found in the vmxnet3 NIC emulator of the QEMU for versions up to v5.2.0. It may occur if a g

Risk And Classification

Problem Types: CWE-190

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
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.d
[SECURITY] [DLA 2623-1] qemu security update	MLIST	lists.d
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	securi
1922441 – (CVE-2021-20203) CVE-2021-20203 qemu: Failed malloc in vmxnet3_activate_device() in hw/net/vmxnet3.c	MISC	bugzil
Bug #1913873 "QEMU: net: vmxnet: integer overflow may crash gues..." : Bugs : QEMU	MISC	bugs.l
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159638 Oracle Enterprise Linux Security Update for qemu (ELSA-2022-9123)
159672 Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2022-9172)
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)
180995 Debian Security Update for qemu (DLA 3099-1)
184091 Debian Security Update for qemu (CVE-2021-20203)
198683 Ubuntu Security Notification for QEMU Vulnerabilities (USN-5307-1)
502168 Alpine Linux Security Update for qemu
502353 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)
750338 OpenSUSE Security Update for qemu (openSUSE-SU-2021:0363-1)
900236 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
902907 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (3915)

© [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](#)