



# CVE-2021-3544

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

## Summary

<b>CVE</b>	CVE-2021-3544
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-02 14:15:00 UTC
<b>Updated</b>	2022-10-25 20:21:00 UTC
<b>Description</b>	Several memory leaks were found in the virtio vhost-user GPU device (vhost-user-gpu) of QEMU in versions up to and incl

## Risk And Classification

**Problem Types:** CWE-401

## 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>	11.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All

## References

Reference	Source	Link	Tags
June 2021 QEMU Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
Debian -- Security Information -- DSA-4980-1 qemu	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
oss-security - QEMU: security issues in vhost-user-gpu	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	
1958935 – (CVE-2021-3544) CVE-2021-3544 QEMU: vhost-user-gpu: multiple memory leaks	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159368](#) Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9425)

<a href="#">159465</a> Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9425)
<a href="#">159566</a> Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2021-9568)
<a href="#">178817</a> Debian Security Update for qemu (DSA 4980-1)
<a href="#">182847</a> Debian Security Update for qemu (CVE-2021-3544)
<a href="#">198432</a> Ubuntu Security Notification for QEMU vulnerabilities (USN-5010-1)
<a href="#">198683</a> Ubuntu Security Notification for QEMU Vulnerabilities (USN-5307-1)
<a href="#">502356</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="#">750821</a> OpenSUSE Security Update for qemu (openSUSE-SU-2021:2213-1)
<a href="#">750827</a> OpenSUSE Security Update for qemu (openSUSE-SU-2021:1043-1)
<a href="#">900063</a> CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
<a href="#">903284</a> Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (4342)

© [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](#)