



# CVE-2021-3713

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

## Summary

<b>CVE</b>	CVE-2021-3713
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-25 19:15:00 UTC
<b>Updated</b>	2022-10-25 20:37:00 UTC
<b>Description</b>	An out-of-bounds write flaw was found in the UAS (USB Attached SCSI) device emulation of QEMU in versions prior to 6.2.

## Risk And Classification

**Problem Types:** CWE-787

## 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>	11.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All

## References

Reference	Source	Link
1994640 – (CVE-2021-3713) CVE-2021-3713 QEMU: out-of-bounds write in UAS (USB Attached SCSI) device emulation	MISC	<a href="#">bugz</a>
Debian -- Security Information -- DSA-4980-1 qemu	DEBIAN	<a href="#">www</a>
[SECURITY] [DLA 3099-1] qemu security update	MLIST	<a href="#">lists.</a>
[SECURITY] [DLA 2753-1] qemu security update	MLIST	<a href="#">lists.</a>
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	<a href="#">secu</a>
CVE-2021-3713 QEMU Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">secu</a>
CVE Program record	CVE.ORG	<a href="#">www</a>
NVD vulnerability detail	NVD	<a href="#">nvd.</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

159582 Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9638)
159672 Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2022-9172)
178782 Debian Security Update for qemu (DLA 2753-1)
178817 Debian Security Update for qemu (DSA 4980-1)
180995 Debian Security Update for qemu (DLA 3099-1)
184759 Debian Security Update for qemu (CVE-2021-3713)
198683 Ubuntu Security Notification for QEMU Vulnerabilities (USN-5307-1)
502168 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)
751276 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:3519-1)
751322 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:3614-1)
751323 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:3613-1)
751330 OpenSUSE Security Update for qemu (openSUSE-SU-2021:3614-1)
751332 OpenSUSE Security Update for qemu (openSUSE-SU-2021:3605-1)
751334 OpenSUSE Security Update for qemu (openSUSE-SU-2021:3604-1)
751337 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1461-1)
751338 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:3635-1)
751362 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:3653-1)
900324 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
901894 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (6831)
902094 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (6831-1)
902980 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (5433)

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](#)**