



CVE-2020-25624

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-25624
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-30 07:15:00 UTC
Updated	2022-09-23 15:27:00 UTC
Description	hw/usb/hcd-ohci.c in QEMU 5.0.0 has a stack-based buffer over-read via values obtained from the host controller driver.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Qemu	Qemu	5.0.0	-	All	All
Application	Qemu	Qemu	5.0.0	-	All	All

References

Reference	Source	Link	Tags
CVE-2020-25624 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.debian.org	
[PATCH v2 1/2] hw: usb: hcd-ohci: check len and frame_number variables	MISC	lists.nongnu.org	Exploit, Mailing Lis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[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)
180995 Debian Security Update for qemu (DLA 3099-1)
502352 Alpine Linux Security Update for qemu
750251 OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)

© [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](#)