



# CVE-2020-25084

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

## Summary

<b>CVE</b>	CVE-2020-25084
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-09-25 05:15:00 UTC
<b>Updated</b>	2022-09-23 15:28:00 UTC
<b>Description</b>	QEMU 5.0.0 has a use-after-free in hw/usb/hcd-xhci.c because the usb_packet_map return value is not checked.

## Risk And Classification

**Problem Types:** CWE-416

## 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>	9.0	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>	5.0.0	-	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	5.0.0	-	All	All

## References

Reference	Source	Link	Tags
oss-security - CVE-2020-25084 QEMU: usb: use-after-free issue while setting up packet	CONFIRM	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, Pa
[PULL 01/18] hw: xhci: check return value of 'usb_packet_map'	MISC	<a href="http://lists.nongnu.org">lists.nongnu.org</a>	Mailing List, Pa
[SECURITY] [DLA 3099-1] qemu security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	
[SECURITY] [DLA 2560-1] qemu security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing List, Th
October 2020 QEMU Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="http://security.netapp.com">security.netapp.com</a>	Third Party Adv
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, anal

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](#)