



# CVE-2020-13765

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

## Summary

<b>CVE</b>	CVE-2020-13765
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-04 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:16:00 UTC
<b>Description</b>	rom_copy() in hw/core/loader.c in QEMU 4.0 and 4.1.0 does not validate the relationship between two addresses, which all

## 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="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	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>	4.0.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	4.1.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	4.1.0	All	All	All

## References

Reference	Source	Link
git.qemu.org Git - qemu.git/commit		<a href="#">git.qem</a>
hw/core/loader: Fix possible crash in rom_copy() · qemu/qemu@4f1c6cb · GitHub	MISC	<a href="#">github.</a>
[SECURITY] [DLA 2262-1] qemu security update	MLIST	<a href="#">lists.de</a>
[SECURITY] [DLA 2288-1] qemu security update	MLIST	<a href="#">lists.de</a>
CVE-2020-13765 QEMU Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">securit</a>
USN-4467-1: QEMU vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ub</a>

git.qemu.org Git - qemu.git/commit	MISC	<a href="#">git.qem</a>
oss-security - CVE-2020-13765 QEMU: loader: OOB access while loading registered ROM may lead to code execution	CONFIRM	<a href="#">www.o</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

<a href="#">174921</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)
<a href="#">174922</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1240-1)
<a href="#">174923</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)
<a href="#">174924</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)
<a href="#">174926</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1242-1)
<a href="#">352242</a> Amazon Linux Security Advisory for qemu-kvm: ALAS-2021-1488
<a href="#">352251</a> Amazon Linux Security Advisory for qemu: ALAS2-2021-1617
<a href="#">377426</a> Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2021:0008)
<a href="#">502350</a> Alpine Linux Security Update for qemu

© [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](#)