



# CVE-2016-2198

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

## Summary

<b>CVE</b>	CVE-2016-2198
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-12-29 22:59:00 UTC
<b>Updated</b>	2020-11-10 17:54:00 UTC
<b>Description</b>	QEMU (aka Quick Emulator) built with the USB EHCI emulation support is vulnerable to a null pointer dereference flaw. It c

## Risk And Classification

**Problem Types:** CWE-476

## 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>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc0	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc1	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc2	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc3	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc4	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc0	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc1	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc2	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc3	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.6.0	rc4	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All

## References

Reference	Source	Link	Tags
oss-security - CVE request Qemu: usb: ehci null pointer dereference in ehci_caps_write	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing Lis

[SECURITY] [DLA 1497-1] qemu security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Third Party
oss-security - Re: CVE request Qemu: usb: ehci null pointer dereference in ehci_caps_write	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	Mailing Lis
Bug 1301643 – CVE-2016-2198 Qemu: usb: ehci null pointer dereference in ehci_caps_write	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Trac
[Qemu-devel] [PATCH] usb: ehci: add capability mmio write function	MLIST	<a href="https://lists.gnu.org">lists.gnu.org</a>	Patch, Ver
QEMU: Multiple vulnerabilities (GLSA 201604-01) — Gentoo Security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Third Party
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

[900063](#) CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

© [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](https://status.cve.report)