



CVE-2017-5973

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

Summary

CVE	CVE-2017-5973
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-27 15:59:00 UTC
Updated	2023-11-07 02:49:00 UTC
Description	The xhci_kick_epctx function in hw/usb/hcd-xhci.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	11	All	All	All
Application	Redhat	Openstack	11.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	8	All	All	All
Application	Redhat	Openstack	8.0	All	All	All
Application	Redhat	Openstack	9	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	11.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All

Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	8.0	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference	Source	Link
git.qemu.org Git - qemu.git/commit	CONFIRM	git.qemu-project.org
QEMU 'hw/usb/hcd-xhci.c' Denial of Service Vulnerability	BID	www.securityfocus.com
Red Hat Customer Portal	REDHAT	access.redhat.com
[SECURITY] [DLA 1497-1] qemu security update	MLIST	lists.debian.org
git.qemu.org Git - qemu.git/commit		git.qemu-project.org
[Qemu-devel] [PATCH] xhci: apply limits to loops	MLIST	lists.gnu.org
Red Hat Customer Portal	REDHAT	access.redhat.com
oss-security - CVE-2017-5973 Qemu: usb: infinite loop while doing control transfer in xhci_kick_epctx	MLIST	www.openwall.com
Bug 1421626 – CVE-2017-5973 Qemu: usb: infinite loop while doing control transfer in xhci_kick_epctx	CONFIRM	bugzilla.redhat.com
QEMU: Multiple vulnerabilities (GLSA 201704-01) — Gentoo Security	GENTOO	security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710523](#) Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201704-01)

[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