



# CVE-2017-8112

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

## Summary

<b>CVE</b>	CVE-2017-8112
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-02 14:59:00 UTC
<b>Updated</b>	2020-09-10 17:30:00 UTC
<b>Description</b>	hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (ir

## Risk And Classification

**Problem Types:** CWE-835

## 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>	All	All	All	All

## References

Reference	Source	Link	Tags
Bug 1445621 – CVE-2017-8112 Qemu: scsi: vmw_pvscsi: infinite loop in pvscsi_log2	CONFIRM	<a href="#">bugzilla.redhat.com</a>	Issue Tracking
QEMU CVE-2017-8112 Denial of Service Vulnerability	BID	<a href="#">www.securityfocus.com</a>	Third Party Ad
[SECURITY] [DLA 1497-1] qemu security update	MLIST	<a href="#">lists.debian.org</a>	Mailing List, Tr
oss-security - CVE-2017-8112 Qemu: scsi: vmw_pvscsi: infinite loop in pvscsi_log2	MLIST	<a href="#">www.openwall.com</a>	Mailing List, Tr
QEMU: Multiple vulnerabilities (GLSA 201706-03) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>	Third Party Ad
Re: [Qemu-devel] [PATCH] vmw_pvscsi: check message ring page count at in	MLIST	<a href="#">lists.gnu.org</a>	Mailing List, Pa
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, ana

No vendor comments have been submitted for this CVE.

710528 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201706-03)

© [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](#)**