



# CVE-2016-10155

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2016-10155
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-15 15:59:00 UTC
<b>Updated</b>	2023-11-07 02:29:00 UTC
<b>Description</b>	Memory leak in hw/watchdog/wdt_i6300esb.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cau:

## Risk And Classification

**Problem Types:** CWE-401

## 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
QEMU: Multiple vulnerabilities (GLSA 201702-28) — Gentoo Security	GENTOO	<a href="#">security.gentoo.org</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
[SECURITY] [DLA 1497-1] qemu security update	MLIST	<a href="#">lists.debian.org</a>
git.qemu.org Git - qemu.git/commit		<a href="#">git.qemu.org</a>
oss-security - CVE request Qemu: watchdog: memory leakage in virtual hardware watchdog wdt_i6300esb	MLIST	<a href="#">www.openwall.com</a>
oss-security - Re: CVE request Qemu: watchdog: memory leakage in virtual hardware watchdog wdt_i6300esb	MLIST	<a href="#">www.openwall.com</a>
git.qemu.org Git - qemu.git/commit	CONFIRM	<a href="#">git.qemu.org</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
QEMU CVE-2016-10155 Denial of Service Vulnerability	BID	<a href="#">www.securityfocus.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710393](#) Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201702-28)

[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](#)