



# CVE-2016-9103

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

## Summary

<b>CVE</b>	CVE-2016-9103
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-12-09 22:59:00 UTC
<b>Updated</b>	2023-02-12 23:27:00 UTC
<b>Description</b>	The v9fs_xattrcreate function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to obtain

## Risk And Classification

**Problem Types:** CWE-200

## 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
[SECURITY] [DLA 1599-1] qemu security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing List, Third Par
QEMU: Multiple vulnerabilities (GLSA 201611-11) — Gentoo Security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Third Party Advisory
oss-security - Re: CVE request Qemu: 9pfs: information leakage via xattribute	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	Mailing List, Third Par
QEMU 'hw/9pfs/9p.c' Information Disclosure Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory,
git.qemu.org Git - qemu.git/commit	CONFIRM	<a href="https://git.qemu.org">git.qemu.org</a>	Patch, Vendor Adviso
git.qemu.org Git - qemu.git/commit	MISC	<a href="https://git.qemu.org">git.qemu.org</a>	
oss-security - CVE request Qemu: 9pfs: information leakage via xattribute	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	Mailing List, Third Par
Re: [Qemu-devel] [PATCH 1/2] 9pfs: fix information leak in xattr read	MLIST	<a href="https://lists.gnu.org">lists.gnu.org</a>	Patch, Third Party Ad
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, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[501229](#) Alpine Linux Security Update for qemu

[505339](#) 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](#)**