



# CVE-2016-9602

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

## Summary

<b>CVE</b>	CVE-2016-9602
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-04-26 19:29:00 UTC
<b>Updated</b>	2023-11-07 02:37:00 UTC
<b>Description</b>	Qemu before version 2.9 is vulnerable to an improper link following when built with the VirtFS. A privileged user inside gues

## Risk And Classification

### Problem Types: CWE-59

## 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
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All

## References

### Reference

QEMU Symbolic Link Flaw in Plan 9 FS Support Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - Security
[SECURITY] [DLA 1497-1] qemu security update
[Qemu-devel] [PATCH RFC 00/36] 9pfs: local: fix vulnerability to symlink
oss-security - CVE-2016-9602 Qemu: 9p: virtfs allows guest to access host filesystem
QEMU CVE-2016-9602 Privilege Escalation Vulnerability
QEMU: Multiple vulnerabilities (GLSA 201704-01) — Gentoo Security
1413929 - (CVE-2016-9602) CVE-2016-9602 Qemu: 9p: virtfs allows guest to access host filesystem
[Qemu-devel] [PATCH 00/29] 9pfs: local: fix vulnerability to symlink att
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

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

© [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](#)