CVE-2016-9602

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-9602
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-26 19:29:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	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	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
Application	Qemu	Qemu	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)