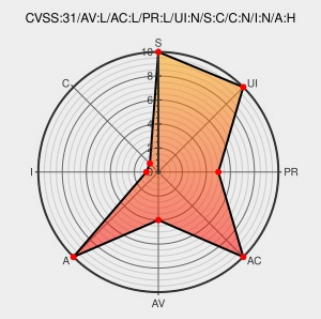
CVE-2020-10717

Published on: 05/04/2020 12:00:00 AM UTC

Last Modified on: 11/16/2022 03:25:00 AM UTC

CVE-2020-10717

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Qemu from Qemu contain the following vulnerability:

A potential DoS flaw was found in the virtio-fs shared file system daemon (virtiofsd) implementation of the QEMU version >= v5.0. Virtio-fs is meant to share a host file system directory with a guest via virtio-fs device. If the guest opens the maximum number of file descriptors under the shared directory, a denial of service may occur. This flaw allows a guest user/process to cause this denial of service on the host.

CVE-2020-10717 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **The QEMU Project** - **QEMU** version **>= QEMU v5.0**

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	NONE	HIGH

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link

oss-security - CVE-2020-10717 QEMU: virtiofsd: guest may open maximum file descriptor to cause DoS	www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2020/05/04/1
1827808 – (CVE-2020-10717) CVE-2020-10717 QEMU: virtiofsd: guest may open maximum file descriptor to cause DoS	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10717
[PULL 0/6] virtiofs queue	lists.gnu.org text/html	MISC lists.gnu.org/archive/html/qemu-devel/2020-05/msg00141.html
QEMU: Multiple vulnerabilities (GLSA 202011-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202011-09
[PULL 2/6] virtiofsd: stay below fs.file-max sysctl value (CVE-2020-1071	lists.gnu.org text/x-diff	MISC lists.gnu.org/archive/html/qemu-devel/2020-05/msg00143.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	All	All	All	All

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→