Date: Fri, 22 Jan 2021 13:42:27 +0530 (IST)
From: P J P <ppandit@...hat.com>
To: oss security list <oss-security@...ts.openwall.com>
cc: Alex Xu <alex@...u.ca>, Stefan Hajnoczi <shajnocz@...hat.com>
Subject: CVE-2020-35517 QEMU: virtiofsd: potential privileged host device access from guest

Hello,

A potential host privilege escalation issue was found in the virtio-fs shared file system daemon (virtiofsd) of the QEMU. Virtio-fs daemon shares host directory tree with a guest VM. The said privilege escalation scenario may occur if a privileged guest user was to create device special file in the shared directory and use it to r/w access host devices. A privileged guest user may use this flaw to arbitrarily access (r/w) host files resulting in DoS scenario or may potentially escalate privileges on the host.

Upstream patch:

-> https://lists.gnu.org/archive/html/qemu-devel/2021-01/msg05461.html

* This issue was reported by Alex Xu (CC'd).

* 'CVE-2020-35517' assigned by Red Hat Inc.

Thank you.
--
Prasad J Pandit / Red Hat Product Security Team
8685 545E B54C 486B C6EB 271E E285 8B5A F050 DE8D