Bug 1908004 (CVE-2020-14394) - CVE-2020-14394 QEMU: infinite loop in xhci_ring_chain_length() in hw/usb/hcd-xhci.c

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-14394
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: low
Severity: low
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact:
Docs Contact:
URL:
Whiteboard:
Depends On: 1908051 ~~1908050~~ 1908054 1908055 1908056 1910659
Blocks: 1896917 1939870
TreeView+ depends on / blocked

Reported: 2020-12-15 16:32 UTC by Mauro Matteo Cascella
Modified: 2022-11-30 16:50 UTC (History)
CC List: 35 users (show)
Fixed In Version: qemu-kvm 7.1.0
Doc Type: If docs needed, set a value
Doc Text: An infinite loop flaw was found in the USB xHCI controller emulation of QEMU while computing the length of the Transfer Request Block (TRB) Ring. This flaw allows a privileged guest user to hang the QEMU process on the host, resulting in a denial of service. The highest threat from this vulnerability is to system availability.
Clone Of:
Environment:
Last Closed: 2021-10-28 11:00:36 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Mauro Matteo Cascella 2020-12-15 16:32:14 UTC — Description

An infinite loop issue was found in the USB xHCI controller emulation of QEMU. Specifically, function xhci_ring_chain_length() in hw/usb/hcd-xhci.c may get stuck while fetching TRBs from guest memory, since the exit conditions of the loop depend on values that are fully controlled by guest. A privileged guest user may exploit this issue to hang the QEMU process on the host, resulting in a denial of service.

Mauro Matteo Cascella 2020-12-15 18:22:33 UTC — Comment 3

Created qemu tracking bugs for this issue:

Affects: epel-7 [bug 1908051]
Affects: fedora-all [~~bug 1908050~~]

Mauro Matteo Cascella 2020-12-17 15:07:17 UTC — Comment 5

In reply to comment #0:
> Specifically, function xhci_ring_chain_length() in hw/usb/hcd-xhci.c
> may get stuck while fetching TRBs from guest memory, since the exit
> conditions of the loop depend on values that are fully controlled by guest.

To be more precise, xhci_ring_chain_length() is responsible for computing the size of the Transfer Request Block (TRB) Ring by repeatedly fetching TRBs from the 'dequeue' pointer.

Mauro Matteo Cascella 2020-12-17 16:18:06 UTC — Comment 6

Statement:

This flaw has been rated as having a security impact of Low, and is not currently planned to be addressed in future updates of Red Hat Enterprise Linux 7. Red Hat Enterprise Linux 7 is now in Maintenance Support 2 Phase of the support and maintenance life cycle. For additional information, refer to the Red Hat Enterprise Linux Life Cycle: https://access.redhat.com/support/policy/updates/errata/.

Mauro Matteo Cascella 2020-12-21 13:47:53 UTC — Comment 7

Acknowledgments:

Name: Gaoning Pan (Ant Security Light-Year Lab), Xingwei Li (Ant Security Light-Year Lab)

Salvatore Bonaccorso 2021-09-03 12:48:14 UTC — Comment 12

Was this issue brought to upstream? (it's low impact but according to several cross-distro bugzilla it seems to somehow has stalled as bugreport to upstream or was not discussed with qemu-devel)? Any idea?

~~Philippe Mathieu-Daudé~~ 2021-09-03 13:11:24 UTC — Comment 13

(In reply to Salvatore Bonaccorso from comment #12)
> Was this issue brought to upstream? (it's low impact but according to
> several cross-distro bugzilla it seems to somehow has stalled as bugreport
> to upstream or was not discussed with qemu-devel)? Any idea?

I don't recall this being discussed upstream.

Mauro Matteo Cascella 2021-09-03 16:03:27 UTC — Comment 15

In reply to comment #12:
> Was this issue brought to upstream? (it's low impact but according to
> several cross-distro bugzilla it seems to somehow has stalled as bugreport
> to upstream or was not discussed with qemu-devel)? Any idea?

I don't think it was. I'm not sure why it got stuck, but I can open a new issue to bring this up.

Mauro Matteo Cascella 2021-09-28 12:51:25 UTC Comment 18

Upstream issue: https://gitlab.com/qemu-project/qemu/-/issues/646.

Mauro Matteo Cascella 2022-11-30 16:50:09 UTC Comment 20

Upstream commit:
https://gitlab.com/qemu-project/qemu/-/commit/effaf5a240e03020f4ae953e10b764622c3e87cc