Bug 1951118 (CVE-2021-3507) - CVE-2021-3507 QEMU: fdc: heap buffer overflow in DMA read data transfers

Keywords: Security ×

Status: CLOSED ERRATA
Alias: CVE-2021-3507
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: ~~1951475~~ 1951521 1951522 1951523 1951524 1951525 ~~1960575~~
Blocks: 1948986 1951190
TreeView+ depends on / blocked

Reported: 2021-04-19 16:50 UTC by Mauro Matteo Cascella
Modified: 2022-12-04 22:27 UTC (History)
CC List: 30 users (show)
Fixed In Version:
Doc Type: If docs needed, set a value
Doc Text: A heap buffer overflow was found in the floppy disk emulator of QEMU. It could occur in fdctrl_transfer_handler() in hw/block/fdc.c while processing DMA read data transfers from the floppy drive to the guest system. A privileged guest user could use this flaw to crash the QEMU process on the host resulting in DoS scenario, or potential information leakage from the host memory.
Clone Of:
Environment:
Last Closed: 2022-12-04 22:27:42 UTC

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

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2022:7472	0	None	None	None	2022-11-08 09:13:51 UTC
Red Hat Product Errata	RHSA-2022:7967	0	None	None	None	2022-11-15 09:49:57 UTC

Mauro Matteo Cascella 2021-04-19 16:50:57 UTC — Description

A heap buffer overflow was found in the floppy disk emulator of QEMU up to 6.0.0 (including). It could occur in fdctrl_transfer_handler() in hw/block/fdc.c while processing DMA read data transfers from the floppy drive to the guest system. A privileged guest user could use this flaw to crash the QEMU process on the host resulting in DoS scenario, or potential information leakage from the host memory.

Mauro Matteo Cascella 2021-04-19 17:54:15 UTC — Comment 2

Created qemu tracking bugs for this issue:

Affects: fedora-all [~~bug 1951475~~]

Mauro Matteo Cascella 2021-04-20 08:23:49 UTC — Comment 3

The data length is not properly computed/sanitized while processing DMA read data transfers from the floppy drive (specifically, while handling a VERIFY command). This leads a negative value to be used as the data length in fdctrl_transfer_handler(), and eventually used in a memcpy in flatview_write_continue().

Mauro Matteo Cascella 2021-04-20 08:30:27 UTC — Comment 4

```
Stacktrace:
==22918==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61900003c800 at pc 0x555558170177 bp 0x7fffffffbc10 sp 0x7fffffffb3d8
READ of size 786432 at 0x61900003c800 thread T0
#0 0x555558170176 in __asan_memcpy (system-i386+0x2c1c176)
#1 0x55555964a3ed in flatview_write_continue softmmu/physmem.c:2781:13
#2 0x55555963fde8 in flatview_write softmmu/physmem.c:2816:14
#3 0x55555963fde8 in address_space_write softmmu/physmem.c:2908:18
#4 0x555558dcb0e0 in cpu_physical_memory_write master/include/exec/cpu-common.h:80:5
#5 0x555558dcb0e0 in i8257_dma_write_memory hw/dma/i8257.c:452:9
#6 0x555558fdb4d9 in fdctrl_transfer_handler hw/block/fdc.c:1809:13
#7 0x555558fc7377 in fdctrl_write_data hw/block/fdc.c:2459:13
#8 0x555558fc7377 in fdctrl_write hw/block/fdc.c:967:9
[...]

Debug output:
FLOPPY: init controller
FLOPPY: revalidate
FLOPPY: No drive connected
FLOPPY: revalidate
FLOPPY: No drive connected
FLOPPY: revalidate
FLOPPY: Floppy disk (2 h 80 t 18 s) rw
FLOPPY: reset controller
FLOPPY: recalibrate
FLOPPY: recalibrate
FLOPPY: try to read 0 00 01 (max=1 0 00 00)
[R +0.025666] outl 0x9 0x0a0206
FLOPPY: Not in DMA transfer mode !
[...]
[R +0.025798] outw 0x3f4 0x0
fdc_ioport_write write reg 0x04 val 0x00
FLOPPY: select rate register set to 0x00
fdc_ioport_write write reg 0x05 val 0x00
FLOPPY: fdctrl_write_data: 00
FLOPPY: VERIFY command
FLOPPY: Calling handler for 'VERIFY'
FLOPPY: Start transfer at 0 0 00 02 (1)
FLOPPY: direction=5 (8704 - -512)
FLOPPY: copy -512 bytes (-512 0 -512) 0 pos 0 00 (2-0x00000001 0x00000200)
FLOPPY: copy 1 bytes (1 0 -512) 0 pos 0 00 (2-0x00000001 0x00000200)
FLOPPY: end transfer 1 1 -512
FLOPPY: transfer status: 00 00 00 (00)
```

FLOPPY: Set interrupt status to 0x00

Mauro Matteo Cascella 2021-04-22 08:08:24 UTC Comment 7

Statement:

This issue affects the version of `qemu-kvm` as shipped with Red Hat Enterprise Linux 8 and Red Hat Enterprise Linux 8 Advanced Virtualization. A future update may address this flaw.

Mauro Matteo Cascella 2021-05-13 08:05:50 UTC Comment 8

Acknowledgments:

Name: Alexander Bulekov

Mauro Matteo Cascella 2021-05-14 09:29:23 UTC Comment 9

Created xen tracking bugs for this issue:

Affects: fedora-all [~~bug 1960575~~]

Salvatore Bonaccorso 2021-09-03 13:04:46 UTC Comment 10

Has this issue been forwarded to upstream?

Mauro Matteo Cascella 2021-09-03 17:55:59 UTC Comment 11

In reply to comment #10:
> Has this issue been forwarded to upstream?

Yes, this was notified upstream. The patch should still be in the works.

Hi John, iirc this was going to be addressed together with the NULL pointer issues tracked here: https://gitlab.com/qemu-project/qemu/-/issues/338. The fixes for those CVEs still need to be applied. Do you have any updates about this? Thanks.

[1] CVE-2020-25741: https://lists.nongnu.org/archive/html/qemu-devel/2020-09/msg07779.html
[2] CVE-2021-20196: https://lists.nongnu.org/archive/html/qemu-devel/2021-01/msg05986.html

John Snow 2021-09-13 15:39:59 UTC Comment 12

(In reply to Mauro Matteo Cascella from comment #11)
> In reply to comment #10:
> > Has this issue been forwarded to upstream?
> >
> Yes, this was notified upstream. The patch should still be in the works.
> >
> Hi John, iirc this was going to be addressed together with the NULL pointer
> issues tracked here: https://gitlab.com/qemu-project/qemu/-/issues/338. The
> fixes for those CVEs still need to be applied. Do you have any updates about
> this? Thanks.
> >
> [1] CVE-2020-25741:
> https://lists.nongnu.org/archive/html/qemu-devel/2020-09/msg07779.html
> [2] CVE-2021-20196:
> https://lists.nongnu.org/archive/html/qemu-devel/2021-01/msg05986.html

Adding to my urgent list alongside the other AHCI and FDC bugs. Will report back soon. From memory, we have fixes but I was thinking that they would be re-sent to list, but they seem to have been lost in the shuffle. Allow me to track down where the ball got dropped and I'll push on these.

--js

Klaus Heinrich Kiwi 2022-01-17 14:18:07 UTC Comment 14

John/Jon - any news about this? We need to decide what to do on downstream RHEL-8.6 (there's also an -AV bug which I think it's moot but necessary due to the z-stream process) and RHEL-9

Thomas Huth 2022-05-12 18:11:35 UTC Comment 20

Kevin just merged Philippe's fix here:
https://gitlab.com/qemu-project/qemu/-/commit/defac5e2fbddf8423a354ff0454283a2115e1367
https://gitlab.com/qemu-project/qemu/-/commit/46609b90d9e3a6304def11038a76b58ff43f77bc

errata-xmlrpc 2022-11-08 09:13:48 UTC Comment 21

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2022:7472 https://access.redhat.com/errata/RHSA-2022:7472

errata-xmlrpc 2022-11-15 09:49:54 UTC Comment 22

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2022:7967 https://access.redhat.com/errata/RHSA-2022:7967

Product Security DevOps Team 2022-12-04 22:27:39 UTC Comment 23

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2021-3507

Note

You need to log in before you can comment on or make changes to this bug.