QEMU

Overview Code Bugs Blueprints Translations Answers

Fix Released

## QEMU: scsi: use-after-free in mptsas\_process\_scsi\_io\_request() of mptsas1068 emulator

Bug #1914236 reported by P J P on 2021-02-02

This bug affects 1 person 25

Affects Status Importance Assigned to Milestone

Unassigned

Undecided

QEMU	Fix Released		Undecided
Bug Description			
* Cheolwoo Myung of issue in the SCSI emulator of the		y reported a use-a	fter-free
* It occurs while	handling mptsas_process_sc	si_io_request(), a	s it does
check a list in	s->pending.		
* This was found i	n version 5.2.0 (master)		
0x60c000107568 at WRITE of size 8 at	dressSanitizer: heap-use-a pc 0x564514950c7c bp 0x7ff 0x60c000107568 thread TO in mptsas process_scsi_io_	f524ef4b0 sp 0x7ff	f524ef4a0
c:306	in mptsas fetch request		
#2 0x564514950c7b	in mptsas_fetch_requests . in aio_bh_poll/util/asy	./hw/scsi/mptsas.c	
	in aio_dispatch/util/ai		
	in aio_ctx_dispatch/uti		
	<pre>in g_main_context_dispatch inux-gnu/libglib-2.0.so.0+</pre>		
#7 0x56451583f059	in glib_pollfds_poll/ut	il/main-loop.c:221	
	in os_host_main_loop_wait		c:244
	in main_loop_wait/util/ in qemu_main_loop/soft		
#11 0x5645143ddd3d	in main/softmmu/main.c		
	inlibc_start_main -gnu/libc.so.6+0x21b96)		
#13 0x5645143eece9			
	/hyfuzz/src/qemu-repro/bui	ld/qemu-system-i38	6+0x1d55ce9)
	located 104 bytes inside o	f 120-byte region	
[0x60c000107500,0x freed by thread T0			
	ininterceptor_free		
(/usr/lib/x86_64-1	inux-gnu/libasan.so.4+0xde		
#1 0x56451495008b c:358	in mptsas_process_scsi_io_	request/hw/scsi	/mptsas.
	in mptsas_fetch_request		
#3 0x56451495008b #4 0x7fff524ef8bf	in mptsas_fetch_requests . ( <unknown module="">)</unknown>	./hw/scsi/mptsas.c	:790
#0 0x7f1cca977d28 (/usr/lib/x86_64-1 #1 0x7f1cc8af9b10	ed by thread TO here: ininterceptor_calloc inux-gnu/libasan.so.4+0xde in g_malloc0 inux-gnu/libglib-2.0.so.0+		
	( <unknown module="">)</unknown>		
	nitizer: heap-use-after-fr	ee/hw/scsi/mpts	as.c:306
in mptsas_process_ Shadow bytes aroun	scsi_io_request d the buggy address:		
	fa fa fa fa fa fa fa fd f	d fd fd fd fd f	d
	fd fd fd fd fd fd fa f		
	fd fd fd fd fd fd fd fd f fa fa fa fa fa fa fa fd f		
0x0c1880018e90: fc	fd fd fd fd fd fd fa f	a fa fa fa fa f	a
	fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa 00 0		
	00 00 00 00 00 00 fa fa f		
	fa fa fa fa fa fa fa fa f		
	fa f		
	(one shadow byte represen		
Addressable: 00			
Partially addressa Heap left redzone:	ble: 01 02 03 04 05 06 07		
Freed heap region:			
Stack left redzone			
Stack mid redzone: Stack right redzon			
Stack after return			
Stack use after so			
Global redzone: f9 Global init order:			
Poisoned by user:			
Container overflow	: fc		
Array cookie: ac Intra object redzo	ne: bb		
ASan internal: fe			
Left alloca redzon			
Right alloca redzo ==31872==ABORTING	ne: cb		
To reproduce this line.	issue, please run the QEMU	with the followin	g command
iine.			

 $\sharp$  To enable ASan option, please set configuration with the following command  $\$ \ ./configure \ --target-list=i386-softmmu \ --disable-werror \ --enable-$ 

```
Report a bug
  This report contains Public Security information
Everyone can see this security related information.
You are not directly subscribed to this bug's
notifications.
  Edit bug mail
Other bug subscribers
  Subscribe someone else
Notified of all changes
   Paolo Bonzini
May be notified
  Alexander Nevench...
   Anthony Liguori
  Chun-Hung Chen
  Daniel Tai
  Haochen Zhang
  Julio Faracco
  Liang Yan
  Michael Rowland H...
  QiangGuan
  Richard Zhang
  Spencer Yu
  Thomas Bergmann
  ZhiQiang Yan
  copacule
  guangming liu
  hotdigi
  liaoxiaojun
```

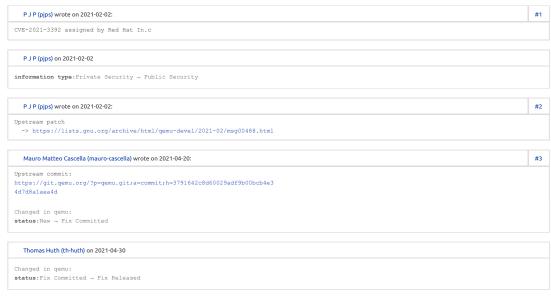
longxingmiao qemu-devel-ml superleaf1995 vrozenfe wangzhh wlfightup sanitizers \$ make

# To reproduce this issue, please run the QEMU process with the
following command line.
\$ ./qemu-system-i386 -m 512 -drive
file=./hyfuzz.img,index=0,media=disk,format=raw -device
mptsas1069,id=scsi -device scsi-hd,drive=SysDisk -drive
id=SysDisk,if=none,file=./disk.img

Tags: cve security

## **CVE References**

2021-3392



To post a comment you must log in.

See full activity log

Launchpad • Take the tour • Read the guide

© 2004-2022 Canonical Ltd. • Terms of use • Data privacy • Contact Launchpad Support • Blog • Careers • System status • 31c7876 (Get the code!)