Closed Issue created 7 months ago by Mauro Matteo Cascella

LSI SCSI Use After Free (CVE-2022-0216)

A use-after-free vulnerability was found in the LSI53C895A SCSI Host Bus Adapter. The flaw occurs while processing repeated messages to cancel the current SCSI request via the lsi_do_msgout function. A malicious privileged user within the guest could use this flaw to crash the QEMU process on the host. Crash is the most likely outcome from this bug (that is, the UAF is not exploitable). See STAR Labs security advisory [1] for more information.

[1] https://starlabs.sg/advisories/22-0216/

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Activity

Thomas Huth added Security Storage labels 7 months ago

Thomas Huth @thuth · 7 months ago Reporter

Maybe this could be fixed with a patch like this?

```
diff a/hw/scsi/lsi53c895a.c b/hw/scsi/lsi53c895a.c
--- a/hw/scsi/lsi53c895a.c
+++ b/hw/scsi/lsi53c895a.c
@@ -1028,8 +1028,9 @@ static void lsi_do_msgout(LSIState *s)
         case 0x0d:
             /* The ABORT TAG message clears the current I/O process only. */
             trace_lsi_do_msgout_abort(current_tag);
-            if (current_req) {
+            if (current_req && current_req->req) {
                 scsi_req_cancel(current_req->req);
+                current_req->req = NULL;
             }
             lsi_disconnect(s);
             break;
```

Mauro Matteo Cascella @mauromatteo.cascella · 4 months ago Author

I do not have a reproducer for testing, but the patch looks good to me. Are you going to post it to qemu-devel? Or I can do that if you prefer. Thanks.

Thomas Huth @thuth · 4 months ago Reporter

I also don't have a reproducer, nor some test environment for the LSI device. But if you feel confident, please go ahead and send it as a proper patch!

juanpc2018 @juanpc2018 · 4 months ago

read this, and could Not resist:

The best SCSI-320 PCIe & PCI-X card from that Era was the ATTO, the only that has Drivers for OSX upto OSX HighSierra 10.13.6, latest OSX and Win drivers can be found in Macrepository or Macgarden, Linux drivers & control SW can be found in a weird blue website "all drivers here".

outdated CD image 2007 from HP can be found in archive.org drivers require a control software to update the firmware, to latest 2009, adjusting scsi settings can be done in the Firmware when updated or control software, but FW menus are more complete.

there was Normal and Low Profile versions, LP version with both Normal an LP brackets was sold rebranded as HP server part: AH627-6000# 1 2 or 3

there are millions, ATTO website No longer has drivers, software for that.

To update the Firmware needs to be done using the Software in Windows8.1x64 preferably "more easy" but Not Bootcamp, real PC board, FW update cannot be done using FW menu, because requires a Real 1.44MB Floppy drive, USB 1.1 floppy wont work, and most boards since 2010 does Not have floppy.

The most expensive/hi-quality/long lasting scsi cables, adapters & terminators were made by Granite Digital, website still works today, but cheaper china cables can be found...

LP version has 2 external channels of VHDI68-Female ports, Normal version also has internal SCSI-320, works well with a 3 meter external VHDI68-male to SCSI-1 Centronix-50-pin cable. SCSI was limited to speed / distance. and active terminator preferably. SCSI does Not terminate to GND like most other devices, terminates between 25% to 50% Vcc, aprox. it requires a low noise voltage regulator, instead of cheaper passive divider resistor networks, for better signal integrity.

LSI was purchased by Broadcom, drivers & control software can be found in the Broadcom website. AQtion was purchased by Marvell, sometimes i mix that.

i have the ATTO if someone need to test. also i have a LSI but... is Not SCSI-320, the next generation PCIe 4GbE SFP Fiber Optic that followed. LSI7204EP, Firmware can be Bios or UEFI, i have the latest UEFI FW installed, but... dont have the external rackmount Hp Storageworks, nor the 4G SFP modules.

that technology was more advanced than SCSI-320 but less popular/common. more obscure abandonware than SCSI-320. 320MB/s = SATA-II, very fast for 2007 - 2009, very slow for today standards. SFP 4Gbe = 500MB/s = SATA-III 6Gbps.

SCSI Control software is required because SCSI Scanners are Async, won't work in HDD mode.

i also have the Firewire400 to SCSI-2 HD-50 adapter from Ratoc FireRex / FR1SX, the advantage of the FireWire dongle is that works Hot-Swap, instead the others Need Reboot when scanner is turned-on. problem is the control software, the free version works in macOS9 or Rosetta in OSX SnowLeopard, and WinXP, there is a $20usd. paid version control software from the Ratoc Japanese website, that works in Vista Only, and has the latest Firmware that is compatible with Vista New PowerSaving mode, nothing more.

Edited by juanpc2018 4 months ago

Alexander Bulekov @a1xndr · 4 months ago Reporter

Guess we should fuzz this device, since CVEs are being assigned

Alexander Bulekov @a1xndr · 4 months ago Reporter

Here's a reproducer for this:

```
cat << EOF | ./qemu-system-i386 -display none -machine accel=qtest, -m \
4G -device lsi53c810,id=scsi -device scsi-hd,drive=disk0 -drive \
file=null-co://,id=disk0,if=none,format=raw -machine q35 -nodefaults  \
-qtest stdio
outl 0xcf8 0x80000810
outl 0xcfc 0xc000
outl 0xcf8 0x80000804
outw 0xcfc 0x05
write 0x69736c10 0x1 0x08
write 0x69736c13 0x1 0x58
write 0x69736c1a 0x1 0x01
write 0x69736c1b 0x1 0x06
write 0x69736c22 0x1 0x01
write 0x69736c23 0x1 0x07
write 0x69736c2b 0x1 0x02
write 0x69736c48 0x1 0x08
write 0x69736c4b 0x1 0x58
write 0x69736c52 0x1 0x04
write 0x69736c53 0x1 0x06
write 0x69736c5b 0x1 0x02
outl 0xc02d 0x697300
write 0x5a554662 0x1 0x01
write 0x5a554663 0x1 0x07
write 0x5a55466a 0x1 0x10
write 0x5a55466b 0x1 0x22
write 0x5a55466c 0x1 0x5a
write 0x5a55466d 0x1 0x5a
write 0x5a55466e 0x1 0x34
write 0x5a55466f 0x1 0x5a
write 0x5a345a5a 0x1 0x77
write 0x5a345a5b 0x1 0x55
write 0x5a345a5c 0x1 0x51
write 0x5a345a5d 0x1 0x27
write 0x27515577 0x1 0x41
outl 0xc02d 0x5a5500
write 0x364001d0 0x1 0x08
write 0x364001d3 0x1 0x58
write 0x364001da 0x1 0x01
write 0x364001db 0x1 0x26
write 0x364001dc 0x1 0x0d
write 0x364001dd 0x1 0xae
write 0x364001de 0x1 0x41
write 0x364001df 0x1 0x5a
write 0x5a41ae0d 0x1 0xf8
write 0x5a41ae0e 0x1 0x36
write 0x5a41ae0f 0x1 0xd7
write 0x5a41ae10 0x1 0x36
write 0x36d736f8 0x1 0x0c
write 0x36d736f9 0x1 0x80
write 0x36d736fa 0x1 0x0d
outl 0xc02d 0x364000
EOF
```

repro.c

Mauro Matteo Cascella mentioned in commit 6c8fa961 4 months ago

Mauro Matteo Cascella closed via commit 6c8fa961 4 months ago

Mauro Matteo Cascella mentioned in commit bonzini/qemu@4367a20c 4 months ago

Mauro Matteo Cascella mentioned in commit frankja/qemu@ae6bb0d3 4 months ago

Please register or sign in to reply