Bug 1966266 (CVE-2021-3582) - CVE-2021-3582 QEMU: pvrdma: unproperly mremap in pvrdma_map_to_pdir()

Keywords: Security ×

Status: CLOSED NOTABUG
Alias: CVE-2021-3582
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: ~~1973144~~
Blocks: 1962562 1968395
TreeView+ depends on / blocked

Reported: 2021-05-31 18:31 UTC by Pedro Sampaio
Modified: 2022-03-25 08:50 UTC (History)
CC List: 27 users (show)
Fixed In Version: qemu 2.17.2
Doc Type: If docs needed, set a value
Doc Text: A flaw was found in the QEMU implementation of VMWare's paravirtual RDMA device. The issue occurs while handling a "PVRDMA_CMD_CREATE_MR" command due to improper memory remapping (mremap). This flaw allows a malicious guest to crash the QEMU process on the host. The highest threat from this vulnerability is to system availability.
Clone Of:
Environment:
Last Closed: 2021-06-17 15:05:24 UTC

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

Pedro Sampaio 2021-05-31 18:31:59 UTC — Description

A flaw was found in QEMU. Because pvrdma unproperly mremap, a VM escape may be caused.

Mauro Matteo Cascella 2021-06-04 11:17:20 UTC — Comment 1

The flaw exists in pvrdma_map_to_pdir() in hw/rdma/vmw/pvrdma_cmd.c. It could occur while handling a 'PVRDMA_CMD_CREATE_MR' command through create_mr() handler, which ultimately calls pvrdma_map_to_pdir. There, mmerap() is called repeatedly in a while loop without properly checking whether the location of the new mapping exceeds a previously remapped memory region.

```
static void *pvrdma_map_to_pdir(...)
{
    ....
    curr_page = rdma_pci_dma_map(pdev, (dma_addr_t)tbl[0], TARGET_PAGE_SIZE);
    ...
    host_virt = mremap(curr_page, 0, length, MREMAP_MAYMOVE);
    ...
    addr_idx = 1;
    while (addr_idx < nchunks) { // nchunks may be > length/TARGET_PAGE_SIZE
    ...
        mremap(curr_page, 0, TARGET_PAGE_SIZE, MREMAP_MAYMOVE | MREMAP_FIXED,
               host_virt + TARGET_PAGE_SIZE * addr_idx); // may remap after host_virt + length
    ...
    addr_idx++;
}
```

Mauro Matteo Cascella 2021-06-17 10:30:17 UTC — Comment 4

Upstream fix:
https://lists.nongnu.org/archive/html/qemu-devel/2021-06/msg04148.html

Mauro Matteo Cascella 2021-06-17 10:31:12 UTC — Comment 5

Created qemu tracking bugs for this issue:

Affects: fedora-all [~~Bug 1973144~~]

Product Security DevOps Team 2021-06-17 15:05:24 UTC — Comment 6

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-2021-3582

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