



author Cindy Lu <lulu@redhat.com> 2023-02-14 16:09:24 +0800
committer Michael S. Tsirkin <mst@redhat.com> 2023-03-10 03:48:27 -0500
commit aed8efddd39b3434c96718d39009285c52b1cafc (patch)
tree b14ce68825b071c263d91ff936d1c283258bdd2d
parent fe15c26ee26efall1741a7b632e9f23b01aca4cc6 (diff)
download linux-aed8efddd39b3434c96718d39009285c52b1cafc.tar.gz

diff options

context: 3
space: include
mode: unified

vp_vdpa: fix the crash in hot unplug with vp_vdpa

While unplugging the vp_vdpa device, it triggers a kernel panic
The root cause is: vdpa_mgmtdev_unregister() will accesses modern
devices which will cause a use after free.
So need to change the sequence in vp_vdpa_remove

```
[ 195.003359] BUG: unable to handle page fault for address: ff4e8beb80199014
[ 195.004012] #PF: supervisor read access in kernel mode
[ 195.004486] #PF: error_code(0x0000) - not-present page
[ 195.004960] PGD 100000067 P4D 1001b6067 PUD 1001b7067 PMD 1001b8067 PTE 0
[ 195.005578] Oops: 0000 1 PREEMPT SMP PTI
[ 195.005968] CPU: 13 PID: 164 Comm: kworker/u56:10 Kdump: loaded Not tainted 5.14.0-252.el9.x86_64 #1
[ 195.006792] Hardware name: Red Hat KVM/RHEL, BIOS edk2-20221207gitffff6d81270b5-2.el9 unknown
[ 195.007556] Workqueue: kacpi_hotplug acpi_hotplug_work_fn
[ 195.008059] RIP: 0010:ioread8+0x31/0x80
[ 195.008418] Code: 77 28 48 81 ff 00 00 01 00 76 0b 89 fa ec 0f b6 c0 c3 cc cc cc cc 8b 15 ad 72 93 01 b8 ff 00 00 00 85 d2 75 0f c3 cc cc cc cc <
[ 195.010104] RSP: 0018:ff4e8beb8067bab8 EFLAGS: 00010292
[ 195.010584] RAX: ffffffff05834a0 RBX: ffffffff05843c0 RCX: ff4e8beb8067bae0
[ 195.011233] RDX: ff1bcbd580f88000 RSI: 0000000000000246 RDI: ff4e8beb80199014
[ 195.011881] RBP: ff1bcbd587e39000 R08: ffffffff916fa2d0 R09: ff4e8beb8067ba68
[ 195.012527] R10: 000000000000001c R11: 0000000000000000 R12: ff1bcbd5a3de9120
[ 195.013179] R13: ffffffff062d000 R14: 0000000000000080 R15: ff1bcbce402bc7805
[ 195.013826] FS: 0000000000000000(0000) GS: ff1bcbce40274000(0000) knlGS:0000000000000000
[ 195.014564] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 195.015093] CR2: ff4e8beb80199014 CR3: 0000000107dea002 CR4: 0000000000771ee0
[ 195.015741] PKRU: 55555554
[ 195.016001] Call Trace:
[ 195.016233] <TASK>
[ 195.016434] vp_modern_get_status+0x12/0x20
[ 195.016823] vp_vdpa_reset+0x1b/0x50 [vp_vdpa]
[ 195.017238] virtio_vdpa_reset+0x3c/0x48 [virtio_vdpa]
[ 195.017709] remove_vq_common+0x1f/0x3a0 [virtio_net]
[ 195.018178] virtnet_remove+0x5d/0x70 [virtio_net]
[ 195.018618] virtio_dev_remove+0x3d/0x90
[ 195.018986] device_release_driver_internal+0x1aa/0x230
[ 195.019466] bus_remove_device+0xd8/0x150
[ 195.019841] device_del+0x18b/0x3f0
[ 195.020167] ? kernfs_find_ns+0x35/0xd0
[ 195.020526] device_unregister+0x13/0x60
[ 195.020894] unregister_virtio_device+0x11/0x20
[ 195.021311] device_release_driver_internal+0x1aa/0x230
[ 195.021790] bus_remove_device+0xd8/0x150
[ 195.022162] device_del+0x18b/0x3f0
[ 195.022487] device_unregister+0x13/0x60
[ 195.022852] ? vdpa_dev_remove+0x30/0x30 [vdpa]
[ 195.023270] vp_vdpa_dev_del+0x12/0x20 [vp_vdpa]
[ 195.023694] vdpa_match_remove+0x2b/0x40 [vdpa]
[ 195.024115] bus_for_each_dev+0x78/0xc0
[ 195.024471] vdpa_mgmtdev_unregister+0x65/0x80 [vdpa]
[ 195.024937] vp_vdpa_remove+0x23/0x40 [vp_vdpa]
[ 195.025353] pci_device_remove+0x36/0xa0
[ 195.025719] device_release_driver_internal+0x1aa/0x230
[ 195.026201] pci_stop_bus_device+0x6c/0x90
[ 195.026580] pci_stop_and_remove_bus_device+0xe/0x20
[ 195.027039] disable_slot+0x49/0x90
[ 195.027366] acpiphp_disable_and_eject_slot+0x15/0x90
[ 195.027832] hotplug_event+0xea/0x210
[ 195.028171] ? hotplug_event+0x210/0x210
[ 195.028535] acpiphp_hotplug_notify+0x22/0x80
[ 195.028942] ? hotplug_event+0x210/0x210
[ 195.029303] acpi_device_hotplug+0x8a/0x1d0
[ 195.029690] acpi_hotplug_work_fn+0x1a/0x30
[ 195.030077] process_one_work+0x1e8/0x3c0
[ 195.030451] worker_thread+0x50/0x3b0
[ 195.030791] ? rescuer_thread+0x3a0/0x3a0
[ 195.031165] kthread+0xd9/0x100
[ 195.031459] ? kthread_complete_and_exit+0x20/0x20
[ 195.031899] ret_from_fork+0x22/0x30
[ 195.032233] </TASK>
```

Fixes: ffbda8e9df10 ("vdpa/vp_vdpa : add vdpa tool support in vp_vdpa")

Tested-by: Lei Yang <leiyang@redhat.com>

Cc: stable@vger.kernel.org

Signed-off-by: Cindy Lu <lulu@redhat.com>

Message-Id: <20230214080924.131462-1-lulu@redhat.com>
Signed-off-by: Michael S. Tsirkin <mst@redhat.com>
Acked-by: Jason Wang <jasowang@redhat.com>

Diffstat

```
-rw-r--r-- drivers/vdpa/virtio_pci/vp_vdpa.c 2
```

1 files changed, 1 insertions, 1 deletions

diff --git a/drivers/vdpa/virtio_pci/vp_vdpa.c b/drivers/vdpa/virtio_pci/vp_vdpa.c

index 8fe267ca3e76f2..281287fae89f13 100644

--- a/drivers/vdpa/virtio_pci/vp_vdpa.c

+++ b/drivers/vdpa/virtio_pci/vp_vdpa.c

@@ -645,8 +645,8 @@ static void vp_vdpa_remove(struct pci_dev *pdev)
struct virtio_pci_modern_device *mdev = NULL;

mdev = vp_vdpa_mgtdev->mdev;
- vp_modern_remove(mdev);
vdpa_mgmtdev_unregister(&vp_vdpa_mgtdev->mgtdev);
+ vp_modern_remove(mdev);
kfree(vp_vdpa_mgtdev->mgtdev.id_table);
kfree(mdev);
kfree(vp_vdpa_mgtdev);