



author Daniil Tatianin <d-tatianin@yandex-team.ru> 2023-03-16 13:29:21 +0300
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-03-30 12:49:04 +0200
commit [97ea704f39b5ded96f071e98701aa543f6f89683](#) (patch)
tree [05d8959a48906f91e7dce79e96e8c71408fc0b89](#)
parent [58c11bc7adaa8c6a369bf1a6baaf213c467073bd](#) (diff)
download [linux-97ea704f39b5ded96f071e98701aa543f6f89683.tar.gz](#)

diff options

context:
space:
mode:

qed/qed_sriov: guard against NULL derefs from qed_iov_get_vf_info

[Upstream commit 25143b6a01d0cc5319edd3de22ffa2578b045550]

We have to make sure that the info returned by the helper is valid before using it.

Found by Linux Verification Center (linuxtesting.org) with the SVACE static analysis tool.

Fixes: [f990c82c385b](#) ("qed*: Add support for ndo_set_vf_trust")

Fixes: [733def6a04bf](#) ("qed*: IOV link control")

Signed-off-by: Daniil Tatianin <d-tatianin@yandex-team.ru>

Reviewed-by: Michal Swiatkowski <michal.swiatkowski@linux.intel.com>

Signed-off-by: David S. Miller <davem@davemloft.net>

Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

```
-rw-r--r-- drivers/net/ethernet/qlogic/qed/qed_sriov.c 5
```

1 files changed, 4 insertions, 1 deletions

```
diff --git a/drivers/net/ethernet/qlogic/qed/qed_sriov.c b/drivers/net/ethernet/qlogic/qed/qed_sriov.c
index 0848b5529d48a4..911509c2b17d5b 100644
```

```
--- a/drivers/net/ethernet/qlogic/qed/qed_sriov.c
```

```
+++ b/drivers/net/ethernet/qlogic/qed/qed_sriov.c
```

```
@@ -4404,6 +4404,9 @@ qed_iov_configure_min_tx_rate(struct qed_dev *cdev, int vfid, u32 rate)
     }
```

```
         vf = qed_iov_get_vf_info(QED_LEADING_HWFN(cdev), (u16)vfid, true);
```

```
+         if (!vf)
```

```
+             return -EINVAL;
```

```
+ 
```

```
         vport_id = vf->vport_id;
```

```
         return qed_configure_vport_wfq(cdev, vport_id, rate);
```

```
@@ -5152,7 +5155,7 @@ static void qed_iov_handle_trust_change(struct qed_hwfn *hwfn)
```

```
     /* Validate that the VF has a configured vport */
```

```
     vf = qed_iov_get_vf_info(hwfn, i, true);
```

```
-     if (!vf->vport_instance)
```

```
+     if (!vf || !vf->vport_instance)
```

```
         continue;
```

```
     memset(&params, 0, sizeof(params));
```

