Date: Tue, 17 Aug 2021 19:52:19 +0800
From: butt3rflyh4ck <butterflyhuangxx@...il.com>
To: mani@...nel.org, "David S. Miller" <davem@...emloft.net>,
Jakub Kicinski <kuba@...nel.org>
Cc: linux-arm-msm@...r.kernel.org, netdev@...r.kernel.org
Subject: Another out-of-bound Read in qrtr_endpoint_post in net/qrtr/qrtr.c

Hi, there is another out-of-bound read in qrtr_endpoint_post in
net/qrtr/qrtr.c in 5.14.0-rc6+ and reproduced.

#analyze
In qrtr_endpoint_post, it would post incoming data from the user, the
'len' is the size of data, the problem is in 'size'.
```
case QRTR_PROTO_VER_1:
if (len < sizeof(*v1))   // just  judge len < sizeof(*v1)
goto err;
v1 = data;
hdrlen = sizeof(*v1);
[...]
size = le32_to_cpu(v1->size);
break;
```
If the version of qrtr proto is QRTR_PROTO_VER_1, hdrlen is
sizeof(qrtr_hdr_v1) and size is le32_to_cpu(v1->size).
```
if (len < sizeof(*v2))  // just judge len < sizeof(*v2)
goto err;
v2 = data;
hdrlen = sizeof(*v2) + v2->optlen;
[...]
size = le32_to_cpu(v2->size);
break;
```
if version of qrtr proto is QRTR_PROTO_VER_2, hdrlen is
sizeof(qrtr_hdr_v2) and size is le32_to_cpu(v2->size).

the code as below can be bypassed.
```
if (len != ALIGN(size, 4) + hdrlen)
goto err;
```
if we set size zero and make 'len' equal to 'hdrlen', the judgement
is bypassed.

```
if (cb->type == QRTR_TYPE_NEW_SERVER) {
/* Remote node endpoint can bridge other distant nodes */
const struct qrtr_ctrl_pkt *pkt = data + hdrlen;

qrtr_node_assign(node, le32_to_cpu(pkt->server.node)); //[1]
}
```
*pkt = data + hdrlen = data + len, so pkt pointer the end of data.
[1]le32_to_cpu(pkt->server.node) could read out of bound.

#crash log:
```
[ 2436.657182][ T8433]
==================================================================
[ 2436.658615][ T8433] BUG: KASAN: slab-out-of-bounds in
qrtr_endpoint_post+0x478/0x5b0
[ 2436.659971][ T8433] Read of size 4 at addr ffff88800ef30a2c by task
qrtr_endpoint_p/8433
[ 2436.661476][ T8433]
[ 2436.661964][ T8433] CPU: 1 PID: 8433 Comm: qrtr_endpoint_p Not
tainted 5.14.0-rc6+ #7
[ 2436.663431][ T8433] Hardware name: QEMU Standard PC (i440FX + PIIX,
1996), BIOS 1.13.0-1ubuntu1 04/01/2014
[ 2436.665220][ T8433] Call Trace:
[ 2436.665870][ T8433]  dump_stack_lvl+0x57/0x7d
[ 2436.666748][ T8433]  print_address_description.constprop.0.cold+0x93/0x334
[ 2436.668054][ T8433]  ? qrtr_endpoint_post+0x478/0x5b0
[ 2436.669072][ T8433]  ? qrtr_endpoint_post+0x478/0x5b0
[ 2436.669957][ T8433]  kasan_report.cold+0x83/0xdf
[ 2436.670833][ T8433]  ? qrtr_endpoint_post+0x478/0x5b0
[ 2436.671780][ T8433]  kasan_check_range+0x14e/0x1b0
[ 2436.672707][ T8433]  qrtr_endpoint_post+0x478/0x5b0
[ 2436.673646][ T8433]  qrtr_tun_write_iter+0x8b/0xe0
[ 2436.674587][ T8433]  new_sync_write+0x245/0x360
[ 2436.675462][ T8433]  ? new_sync_read+0x350/0x350
[ 2436.676353][ T8433]  ? policy_view_capable+0x3b0/0x6d0
[ 2436.677266][ T8433]  ? apparmor_task_setrlimit+0x4d0/0x4d0
[ 2436.678251][ T8433]  vfs_write+0x344/0x4e0
[ 2436.679024][ T8433]  ksys_write+0xc4/0x160
[ 2436.679758][ T8433]  ? __ia32_sys_read+0x40/0x40
[ 2436.680605][ T8433]  ? syscall_enter_from_user_mode+0x21/0x70
[ 2436.681661][ T8433]  do_syscall_64+0x35/0xb0
[ 2436.682445][ T8433]  entry_SYSCALL_64_after_hwframe+0x44/0xae
```
#fix suggestion
'size' should not be zero, it is length of packet, excluding this
header or (excluding this header and optlen).

Regards,
 butt3rflyh4ck.
--
Active Defense Lab of Venustech