author	Michael Chan <michael.chan@broadcom.com>	2022-11-03 19:33:26 -0400
committer	Jakub Kicinski <kuba@kernel.org>	2022-11-04 19:29:02 -0700
commit	6d81ea3765dfa6c8a20822613c81edad1c4a16a0 (patch)	
tree	240c075a6b42b934f53c3ea41ae744abebacce7f	
parent	0cf736a18a1e804037839bd8df9e36f0efdb8745 (diff)	
download	linux-6d81ea3765dfa6c8a20822613c81edad1c4a16a0.tar.gz	

diff options

context: 3

space: include

mode: unified

bnxt_en: Fix possible crash in bnxt_hwrm_set_coal()

```
During the error recovery sequence, the rtnl_lock is not held for the
entire duration and some datastructures may be freed during the sequence.
Check for the BNXT_STATE_OPEN flag instead of netif_running() to ensure
that the device is fully operational before proceeding to reconfigure
the coalescing settings.

This will fix a possible crash like this:

BUG: unable to handle kernel NULL pointer dereference at 0000000000000000
PGD 0 P4D 0
Oops: 0000 [#1] SMP NOPTI
CPU: 10 PID: 181276 Comm: ethtool Kdump: loaded Tainted: G          IOE    --------- -  - 4.18.0-348.el8.x86_64 #1
Hardware name: Dell Inc. PowerEdge R740/0F9N89, BIOS 2.3.10 08/15/2019
RIP: 0010:bnxt_hwrm_set_coal+0x1fb/0x2a0 [bnxt_en]
Code: c2 66 83 4e 22 08 66 89 46 1c e8 10 cb 00 00 41 83 c6 01 44 39 b3 68 01 00 00 0f 8e a3 00 00 00 48 8b 93 c8 00 00 00 49 63 c6 <48> 8b 2c c2 48
RSP: 0018:ffffb11c8dcaba50 EFLAGS: 00010246
RAX: 0000000000000000 RBX: ffff8d168a8b0ac0 RCX: 00000000000000c5
RDX: 0000000000000000 RSI: ffff8d162f72c000 RDI: ffff8d168a8b0b28
RBP: 0000000000000000 R08: b6e1f68a12e9a7eb R09: 0000000000000000
R10: 0000000000000001 R11: 0000000000000037 R12: ffff8d168a8b109c
R13: ffff8d168a8b10aa R14: 0000000000000000 R15: ffffffffc01ac4e0
FS:  00007f3852e4c740(0000) GS:ffff8d24c0080000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 0000000000000000 CR3: 000000041b3ee003 CR4: 00000000007706e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
PKRU: 55555554
Call Trace:
 ethnl_set_coalesce+0x3ce/0x4c0
 genl_family_rcv_msg_doit.isra.15+0x10f/0x150
 genl_family_rcv_msg+0xb3/0x160
 ? coalesce_fill_reply+0x480/0x480
 genl_rcv_msg+0x47/0x90
 ? genl_family_rcv_msg+0x160/0x160
 netlink_rcv_skb+0x4c/0x120
 genl_rcv+0x24/0x40
 netlink_unicast+0x196/0x230
 netlink_sendmsg+0x204/0x3d0
 sock_sendmsg+0x4c/0x50
 __sys_sendto+0xee/0x160
 ? syscall_trace_enter+0x1d3/0x2c0
 ? __audit_syscall_exit+0x249/0x2a0
 __x64_sys_sendto+0x24/0x30
 do_syscall_64+0x5b/0x1a0
 entry_SYSCALL_64_after_hwframe+0x65/0xca
RIP: 0033:0x7f38524163bb

Fixes: 2151fe0830fd ("bnxt_en: Handle RESET_NOTIFY async event from firmware.")
Reviewed-by: Somnath Kotur <somnath.kotur@broadcom.com>
Signed-off-by: Michael Chan <michael.chan@broadcom.com>
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
```

Diffstat

-rw-r--r-- drivers/net/ethernet/broadcom/bnxt/bnxt_ethtool.c 2

1 files changed, 1 insertions, 1 deletions

```
diff --git a/drivers/net/ethernet/broadcom/bnxt/bnxt_ethtool.c b/drivers/net/ethernet/broadcom/bnxt/bnxt_ethtool.c
index f57e524c7e30b9..8cad15c458b396 100644
--- a/drivers/net/ethernet/broadcom/bnxt/bnxt_ethtool.c
+++ b/drivers/net/ethernet/broadcom/bnxt/bnxt_ethtool.c
@@ -162,7 +162,7 @@ static int bnxt_set_coalesce(struct net_device *dev,
        }

 reset_coalesce:
-       if (netif_running(dev)) {
+       if (test_bit(BNXT_STATE_OPEN, &bp->state)) {
                if (update_stats) {
                        rc = bnxt_close_nic(bp, true, false);
                        if (!rc)
```