

author Ivan Vecera <ivecera@redhat.com> 2023-03-09 10:45:09 -0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-03-22 13:28:05 +0100
commit 6e18f66b704bd725196508c1db93bf7338cdc8de (patch)
tree 6968b80a6941cae32e9c08d7310720a689aa271d
parent f0216046aeb817230b79f93d0ecbf81f4431d9f0 (diff)
download linux-6e18f66b704bd725196508c1db93bf7338cdc8de.tar.gz

diff options

context: 3

space: include

mode: unified

i40e: Fix kernel crash during reboot when adapter is in recovery mode

[Upstream commit 7e4f8a0c495413a50413e8c9f1032ce1bc633bae]

If the driver detects during probe that firmware is in recovery mode then i40e_init_recovery_mode() is called and the rest of probe function is skipped including pci_set_drvdata(). Subsequent i40e_shutdown() called during shutdown/reboot dereferences NULL pointer as pci_get_drvdata() returns NULL.

To fix call pci_set_drvdata() also during entering to recovery mode.

Reproducer:
1) Lets have i40e NIC with firmware in recovery mode
2) Run reboot

Result:

```
[ 139.084698] i40e: Intel(R) Ethernet Connection XL710 Network Driver
[ 139.090959] i40e: Copyright (c) 2013 - 2019 Intel Corporation.
[ 139.108438] i40e 0000:02:00.0: Firmware recovery mode detected. Limiting functionality.
[ 139.116439] i40e 0000:02:00.0: Refer to the Intel(R) Ethernet Adapters and Devices User Guide for details on firmware recovery mode.
[ 139.129499] i40e 0000:02:00.0: fw 8.3.64775 api 1.13 nvm 8.30 0x8000b78d 1.3106.0 [8086:1583] [15d9:084a]
[ 139.215932] i40e 0000:02:00.0 enp2s0f0: renamed from eth0
[ 139.223292] i40e 0000:02:00.1: Firmware recovery mode detected. Limiting functionality.
[ 139.231292] i40e 0000:02:00.1: Refer to the Intel(R) Ethernet Adapters and Devices User Guide for details on firmware recovery mode.
[ 139.244406] i40e 0000:02:00.1: fw 8.3.64775 api 1.13 nvm 8.30 0x8000b78d 1.3106.0 [8086:1583] [15d9:084a]
[ 139.329209] i40e 0000:02:00.1 enp2s0f1: renamed from eth0
...
[ 156.311376] BUG: kernel NULL pointer dereference, address: 00000000000006c2
[ 156.318330] #PF: supervisor write access in kernel mode
[ 156.323546] #PF: error_code(0x0002) - not-present page
[ 156.328679] PGD 0 P4D 0
[ 156.331210] Oops: 0002 [#1] PREEMPT SMP NOPTI
[ 156.335567] CPU: 26 PID: 15119 Comm: reboot Tainted: G          E        6.2.0+ #1
[ 156.343126] Hardware name: Abacus electric, s.r.o. - servis@abacus.cz Super Server/H12SSW-iN, BIOS 2.4 04/13/2022
[ 156.353369] RIP: 0010:i40e_shutdown+0x15/0x130 [i40e]
[ 156.358430] Code: c1 fc ff ff 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f 1f 44 00 00 55 48 89 fd 53 48 8b 9f 48 01 00 00 <
[ 156.377168] RSP: 0018:ffffb223c8447d90 EFLAGS: 00010282
[ 156.382384] RAX: ffffffffcc073ee70 RBX: 0000000000000000 RCX: 0000000000000001
[ 156.389510] RDX: 0000000080000001 RSI: 0000000000000246 RDI: ffff95db49988000
[ 156.396634] RBP: ffff95db49988000 R08: ffffffffffffffff R09: ffffffff8bd17d40
[ 156.403759] R10: 0000000000000001 R11: ffffffff8a5e3d28 R12: ffff95db49988000
[ 156.410882] R13: ffffffff89a6fe17 R14: ffff95db49988150 R15: 0000000000000000
[ 156.418007] FS:  00007fe7c0cc3980(0000) GS: ffff95ea8ee80000(0000) knlGS:0000000000000000
[ 156.426083] CS:  0010 DS:  0000 ES:  0000 CR0: 0000000080005003
[ 156.431819] CR2: 00000000000006c2 CR3: 00000003092fc005 CR4: 0000000000770ee0
[ 156.438944] PKRU: 55555554
[ 156.441647] Call Trace:
[ 156.444096] <TASK>
[ 156.446199] pci_device_shutdown+0x38/0x60
[ 156.450297] device_shutdown+0x163/0x210
[ 156.454215] kernel_restart+0x12/0x70
[ 156.457872] __do_sys_reboot+0x1ab/0x230
[ 156.461789] ? vfs_writev+0xa6/0x1a0
[ 156.465362] ? __pfx_file_free_rcu+0x10/0x10
[ 156.469635] ? __call_rcu_common.constprop.85+0x109/0x5a0
[ 156.475034] do_syscall_64+0x3e/0x90
[ 156.478611] entry_SYSCALL_64_after_hwframe+0x72/0xdc
[ 156.483658] RIP: 0033:0x7fe7bfff37ab7
```

Fixes: 4ff0ee1af016 ("i40e: Introduce recovery mode support")
Signed-off-by: Ivan Vecera <ivecera@redhat.com>
Tested-by: Arpana Arland <arpanax.arland@intel.com> (A Contingent worker at Intel)
Signed-off-by: Tony Nguyen <anthony.l.nguyen@intel.com>
Link: <https://lore.kernel.org/r/20230309184509.984639-1-anthony.l.nguyen@intel.com>
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

-rw-r--r-- drivers/net/ethernet/intel/i40e/i40e_main.c 1

1 files changed, 1 insertions, 0 deletions

diff --git a/drivers/net/ethernet/intel/i40e/i40e_main.c b/drivers/net/ethernet/intel/i40e/i40e_main.c
index 3f983d69f10ebe..05f2f5637d3df8 100644

```
--- a/drivers/net/ethernet/intel/i40e/i40e_main.c
+++ b/drivers/net/ethernet/intel/i40e/i40e_main.c
@@ -14823,6 +14823,7 @@ static int i40e_init_recovery_mode(struct i40e_pf *pf, struct i40e_hw *hw)
     int err;
     int v_idx;

+    pci_set_drvdata(pf->pdev, pf);
+    pci_save_state(pf->pdev);

     /* set up periodic task facility */
```