author	Petr Oros <poros@redhat.com>	2023-03-01 21:47:07 +0100
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-03-17 08:48:54 +0100
commit	c813f7a3161481483ae2077651b21bc217c419e0 (patch)	
tree	b71764880419c05efc1eb17b42770370eac9bbb6	
parent	3f14457e1584224f4296af613bbd99deb60b5d91 (diff)	
download	linux-c813f7a3161481483ae2077651b21bc217c419e0.tar.gz	

diff options

context: 3

space: include

mode: unified

ice: copy last block omitted in ice_get_module_eeprom()

```
[ Upstream commit 84cba1840e68430325ac133a11be06bfb2f7acd8 ]

ice_get_module_eeprom() is broken since commit e9c9692c8a81 ("ice:
Reimplement module reads used by ethtool") In this refactor,
ice_get_module_eeprom() reads the eeprom in blocks of size 8.
But the condition that should protect the buffer overflow
ignores the last block. The last block always contains zeros.

Bug uncovered by ethtool upstream commit 9538f384b535
("netlink: eeprom: Defer page requests to individual parsers")
After this commit, ethtool reads a block with length = 1;
to read the SFF-8024 identifier value.

unpatched driver:
$ ethtool -m enp65s0f0np0 offset 0x90 length 8
Offset          Values
------          ------
0x0090:         00 00 00 00 00 00 00 00
$ ethtool -m enp65s0f0np0 offset 0x90 length 12
Offset          Values
------          ------
0x0090:         00 00 01 a0 4d 65 6c 6c 00 00 00 00
$

$ ethtool -m enp65s0f0np0
Offset          Values
------          ------
0x0000:         11 06 06 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0010:         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0020:         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0030:         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0040:         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0050:         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0060:         00 00 00 00 00 00 00 00 00 00 00 00 00 01 08 00
0x0070:         00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00

patched driver:
$ ethtool -m enp65s0f0np0 offset 0x90 length 8
Offset          Values
------          ------
0x0090:         00 00 01 a0 4d 65 6c 6c
$ ethtool -m enp65s0f0np0 offset 0x90 length 12
Offset          Values
------          ------
0x0090:         00 00 01 a0 4d 65 6c 6c 61 6e 6f 78
$ ethtool -m enp65s0f0np0
```

```
    Identifier                                : 0x11 (QSFP28)
    Extended identifier                       : 0x00
    Extended identifier description           : 1.5W max. Power consumption
    Extended identifier description           : No CDR in TX, No CDR in RX
    Extended identifier description           : High Power Class (> 3.5 W) not enabled
    Connector                                 : 0x23 (No separable connector)
    Transceiver codes                         : 0x88 0x00 0x00 0x00 0x00 0x00 0x00 0x00
    Transceiver type                          : 40G Ethernet: 40G Base-CR4
    Transceiver type                          : 25G Ethernet: 25G Base-CR CA-N
    Encoding                                  : 0x05 (64B/66B)
    BR, Nominal                               : 25500Mbps
    Rate identifier                           : 0x00
    Length (SMF,km)                           : 0km
    Length (OM3 50um)                         : 0m
    Length (OM2 50um)                         : 0m
    Length (OM1 62.5um)                       : 0m
    Length (Copper or Active cable)           : 1m
    Transmitter technology                    : 0xa0 (Copper cable unequalized)
    Attenuation at 2.5GHz                     : 4db
    Attenuation at 5.0GHz                     : 5db
    Attenuation at 7.0GHz                     : 7db
    Attenuation at 12.9GHz                    : 10db
    ........
    ....

Fixes: e9c9692c8a81 ("ice: Reimplement module reads used by ethtool")
Signed-off-by: Petr Oros <poros@redhat.com>
Reviewed-by: Jesse Brandeburg <jesse.brandeburg@intel.com>
Tested-by: Jesse Brandeburg <jesse.brandeburg@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/intel/ice/ice_ethtool.c 6

1 files changed, 4 insertions, 2 deletions

```
diff --git a/drivers/net/ethernet/intel/ice/ice_ethtool.c b/drivers/net/ethernet/intel/ice/ice_ethtool.c
index 24001035910e0e..60f73e775beeb6 100644
--- a/drivers/net/ethernet/intel/ice/ice_ethtool.c
+++ b/drivers/net/ethernet/intel/ice/ice_ethtool.c
@@ -3998,6 +3998,8 @@ ice_get_module_eeprom(struct net_device *netdev,
                 * SFP modules only ever use page 0.
                 */
                if (page == 0 || !(data[0x2] & 0x4)) {
+                       u32 copy_len;
+
                        /* If i2c bus is busy due to slow page change or
                         * link management access, call can fail. This is normal.
                         * So we retry this a few times.
@@ -4021,8 +4023,8 @@ ice_get_module_eeprom(struct net_device *netdev,
                        }

                        /* Make sure we have enough room for the new block */
-                       if ((i + SFF_READ_BLOCK_SIZE) < ee->len)
-                               memcpy(data + i, value, SFF_READ_BLOCK_SIZE);
+                       copy_len = min_t(u32, SFF_READ_BLOCK_SIZE, ee->len - i);
+                       memcpy(data + i, value, copy_len);
                }
        }
        return 0;
```