author	Lorenzo Bianconi <lorenzo@kernel.org>	2023-02-23 00:10:25 +0100
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2024-10-17 15:21:29 +0200
commit	dffe86df26aee01a5fc56a175b7a7f157961e370 (patch)	
tree	886020d74cd6422a032c0f820a7ec8c74d6e424b	
parent	25703a3c980e21548774eea8c8a87a75c5c8f58c (diff)	
download	linux-dffe86df26aee01a5fc56a175b7a7f157961e370.tar.gz	

diff options

context: 3

space: include

mode: unified

wifi: mt76: do not run mt76_unregister_device() on unregistered hw

commit 41130c32f3a18fcc930316da17f3a5f3bc326aa1 upstream.

Trying to probe a mt7921e pci card without firmware results in a
successful probe where ieee80211_register_hw hasn't been called. When
removing the driver, ieee802111_unregister_hw is called unconditionally
leading to a kernel NULL pointer dereference.
Fix the issue running mt76_unregister_device routine just for registered
hw.

Link: https://bugs.debian.org/1029116
Link: https://bugs.kali.org/view.php?id=8140
Reported-by: Stuart Hayhurst <stuart.a.hayhurst@gmail.com>
Fixes: 1c71e03afe4b ("mt76: mt7921: move mt7921_init_hw in a dedicated work")
Tested-by: Helmut Grohne <helmut@freexian.com>
Signed-off-by: Lorenzo Bianconi <lorenzo@kernel.org>
Signed-off-by: Kalle Valo <kvalo@kernel.org>
Link: https://lore.kernel.org/r/be3457d82f4e44bb71a22b2b5db27b644a37b1e1.1677107277.git.lorenzo@kernel.org
Signed-off-by: Georg Müller <georgmueller@gmx.net>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

Diffstat

-rw-r--r--	drivers/net/wireless/mediatek/mt76/mac80211.c	8
-rw-r--r--	drivers/net/wireless/mediatek/mt76/mt76.h	1

2 files changed, 9 insertions, 0 deletions

```
diff --git a/drivers/net/wireless/mediatek/mt76/mac80211.c b/drivers/net/wireless/mediatek/mt76/mac80211.c
index 6de13d6414389b..82fce4b1d581be 100644
--- a/drivers/net/wireless/mediatek/mt76/mac80211.c
+++ b/drivers/net/wireless/mediatek/mt76/mac80211.c
@@ -522,6 +522,7 @@ int mt76_register_phy(struct mt76_phy *phy, bool vht,
        if (ret)
                return ret;

+       set_bit(MT76_STATE_REGISTERED, &phy->state);
        phy->dev->phys[phy->band_idx] = phy;

        return 0;
@@ -532,6 +533,9 @@ void mt76_unregister_phy(struct mt76_phy *phy)
 {
        struct mt76_dev *dev = phy->dev;

+       if (!test_bit(MT76_STATE_REGISTERED, &phy->state))
+               return;
+
        mt76_tx_status_check(dev, true);
        ieee80211_unregister_hw(phy->hw);
```

```
        dev->phys[phy->band_idx] = NULL;
@@ -654,6 +658,7 @@ int mt76_register_device(struct mt76_dev *dev, bool vht,
                return ret;

        WARN_ON(mt76_worker_setup(hw, &dev->tx_worker, NULL, "tx"));
+       set_bit(MT76_STATE_REGISTERED, &phy->state);
        sched_set_fifo_low(dev->tx_worker.task);

        return 0;
@@ -664,6 +669,9 @@ void mt76_unregister_device(struct mt76_dev *dev)
 {
        struct ieee80211_hw *hw = dev->hw;

+       if (!test_bit(MT76_STATE_REGISTERED, &dev->phy.state))
+               return;
+
        if (IS_ENABLED(CONFIG_MT76_LEDS))
                mt76_led_cleanup(dev);
        mt76_tx_status_check(dev, true);
```

diff --git a/drivers/net/wireless/mediatek/mt76/mt76.h b/drivers/net/wireless/mediatek/mt76/mt76.h
index 60c9f9c56a4f56..5b03e3b33d5463 100644
--- a/drivers/net/wireless/mediatek/mt76/mt76.h
+++ b/drivers/net/wireless/mediatek/mt76/mt76.h

```
@@ -388,6 +388,7 @@ struct mt76_tx_cb {

 enum {
        MT76_STATE_INITIALIZED,
+       MT76_STATE_REGISTERED,
        MT76_STATE_RUNNING,
        MT76_STATE_MCU_RUNNING,
        MT76_SCANNING,
```