



author Abdun Nihaal <abdun.nihaal@gmail.com> 2025-03-30 16:01:10 +0530
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2025-05-02 07:40:58 +0200
commit [6e4ab3e574c2a335b40fa1f70d1c54fcb58ab33f](#) (patch)
tree [137d391d2e8e0287311e947ad158baff7305bb7f](#)
parent [4a8c29beb8a02b5a0a9d77d608aa14b6f88a6b86](#) (diff)
download [linux-6e4ab3e574c2a335b40fa1f70d1c54fcb58ab33f.tar.gz](#)

diff options

context:
space:
mode:

wifi: at76c50x: fix use after free access in at76_disconnect

[Upstream commit 27c7e63b3cb1a20bb78ed4a36c561ea4579fd7da]

The memory pointed to by priv is freed at the end of at76_delete_device function (using ieee80211_free_hw). But the code then accesses the udev field of the freed object to put the USB device. This may also lead to a memory leak of the usb device. Fix this by using udev from interface.

Fixes: 29e20aa6c6af ("at76c50x-usb: fix use after free on failure path in at76_probe()")
Signed-off-by: Abdun Nihaal <abdun.nihaal@gmail.com>
Link: <https://patch.msgid.link/20250330103110.44080-1-abdun.nihaal@gmail.com>
Signed-off-by: Johannes Berg <johannes.berg@intel.com>
Signed-off-by: Sasha Levin <sasha@kernel.org>

Diffstat

```
-rw-r--r-- drivers/net/wireless/atmel/at76c50x-usb.c 2
```

1 files changed, 1 insertions, 1 deletions

```
diff --git a/drivers/net/wireless/atmel/at76c50x-usb.c b/drivers/net/wireless/atmel/at76c50x-usb.c
index 4042578000331e..706de33d0ed49f 100644
```

```
--- a/drivers/net/wireless/atmel/at76c50x-usb.c
```

```
+++ b/drivers/net/wireless/atmel/at76c50x-usb.c
```

```
@@ -2553,7 +2553,7 @@ static void at76_disconnect(struct usb_interface *interface)
```

```
    wiphy_info(priv->hw->wiphy, "disconnecting\n");
    at76_delete_device(priv);
-   usb_put_dev(priv->udev);
+   usb_put_dev(interface_to_usbdev(interface));
    dev_info(&interface->dev, "disconnected\n");
}
```