author	Alexander Aring <aahringo@redhat.com>	2023-02-16 23:25:04 -0500
committer	Stefan Schmidt <stefan@datenfreihafen.org>	2023-03-02 14:39:48 +0100
commit	6c993779ea1d0cccdb3a5d7d45446dd229e610a3 (patch)	
tree	54c301ced978f09bcf808b6ad6ce1f62f63c007d	
parent	044c8bf78db818b8c726eb47c560e05fbc71e128 (diff)	
download	linux-6c993779ea1d0cccdb3a5d7d45446dd229e610a3.tar.gz	

ca8210: fix mac_len negative array access

```
This patch fixes a buffer overflow access of skb->data if
ieee802154_hdr_peek_addrs() fails.

Reported-by: lianhui tang <bluetlh@gmail.com>
Signed-off-by: Alexander Aring <aahringo@redhat.com>
Link: https://lore.kernel.org/r/20230217042504.3303396-1-aahringo@redhat.com
Signed-off-by: Stefan Schmidt <stefan@datenfreihafen.org>
```

Diffstat

-rw-r--r-- drivers/net/ieee802154/ca8210.c 2

1 files changed, 2 insertions, 0 deletions

```
diff --git a/drivers/net/ieee802154/ca8210.c b/drivers/net/ieee802154/ca8210.c
index e1a569b99e4a6a..0b0c6c0764fe9c 100644
--- a/drivers/net/ieee802154/ca8210.c
+++ b/drivers/net/ieee802154/ca8210.c
@@ -1913,6 +1913,8 @@ static int ca8210_skb_tx(
          * packet
          */
         mac_len = ieee802154_hdr_peek_addrs(skb, &header);
+        if (mac_len < 0)
+                return mac_len;

         secspec.security_level = header.sec.level;
         secspec.key_id_mode = header.sec.key_id_mode;
```