TEW-827DRU

Firmware version

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

Description

```
TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains a command
injection in apply.cgi via the action kick_ban_wifi_mac_allow with the key
'qcawifi.wifi0_vap0.maclist', allowing an authenticated user to run arbitrary
commands on the device.
```

Detial

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

```
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
004292D0                 addiu  $a1, $v0, (aIwprivSAddmacS - 0x4C0000)  # "iwpriv %s addmac %s"
004292D4                 addiu  $a0, $fp, 0xF0+var_4C  # s
004292D8                 addiu  $v1, $fp, 0xF0+var_6C
004292DC                 addiu  $v0, $fp, 0xF0+var_8C
004292E0                 move   $a2, $v1
004292E4                 move   $a3, $v0
004292E8                 la     $v0, sprintf
004292EC                 nop
004292F0                 move   $t9, $v0
004292F4                 jalr   $t9 ; sprintf
004292F8                 nop
004292FC                 lw     $gp, 0xF0+var_E0($fp)
00429300                 addiu  $v0, $fp, 0xF0+var_4C
00429304                 move   $a0, $v0          # command
00429308                 la     $v0, system
0042930C                 nop
00429310                 move   $t9, $v0
00429314                 jalr   $t9 ; system
```