TEW-827DRU

Firmware version

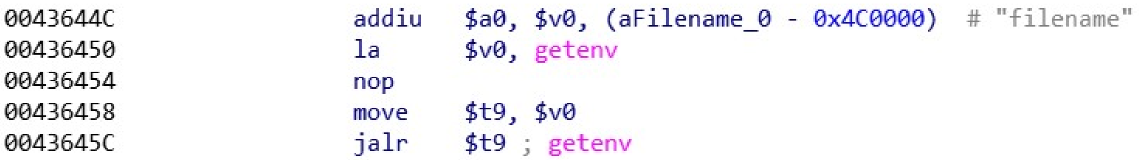
```
TEW-827DRU firmware: 2.06B04
```

Description

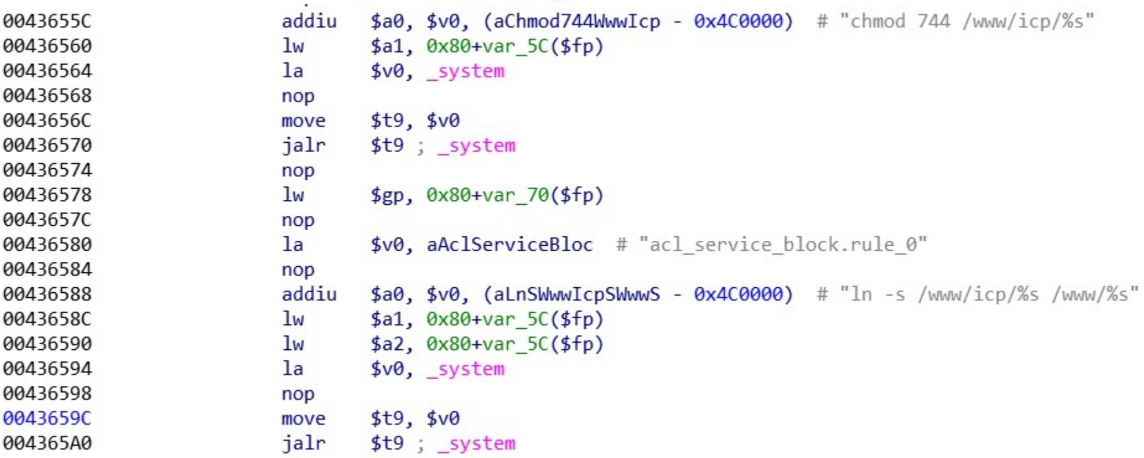
```
TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains multiple
command injections in icp_upload_img.cgi with the key "filename", allowing an
authenticated user to run arbitrary commands on the device.
```

Detial

```
The bug in function: 0x4363A4, binary: www/cgi/ssi
The parameter 'filename' pass to system
```



```
0043644C          addiu   $a0, $v0, (aFilename_0 - 0x4C0000)  # "filename"
00436450          la      $v0, getenv
00436454          nop
00436458          move    $t9, $v0
0043645C          jalr    $t9 ; getenv
```



```
0043655C          addiu   $a0, $v0, (aChmod744WwwIcp - 0x4C0000)  # "chmod 744 /www/icp/%s"
00436560          lw      $a1, 0x80+var_5C($fp)
00436564          la      $v0, _system
00436568          nop
0043656C          move    $t9, $v0
00436570          jalr    $t9 ; _system
00436574          nop
00436578          lw      $gp, 0x80+var_70($fp)
0043657C          nop
00436580          la      $v0, aAclServiceBloc  # "acl_service_block.rule_0"
00436584          nop
00436588          addiu   $a0, $v0, (aLnSWwwIcpSWwwS - 0x4C0000)  # "ln -s /www/icp/%s /www/%s"
0043658C          lw      $a1, 0x80+var_5C($fp)
00436590          lw      $a2, 0x80+var_5C($fp)
00436594          la      $v0, _system
00436598          nop
0043659C          move    $t9, $v0
004365A0          jalr    $t9 ; _system
```