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
wifi_captive_portal_login with the key "REMOTE_ADDR", allowing an authenticated
user to run arbitrary commands on the device.
```

Detial

```
The bug in function: get_mac_from_ip_by_arptable, binary: www/cgi/ssi
```

```
One: The key 'REMOTE_ADDR' pass to system:
```

```
00426CEC                addiu   $v0, (aCatProcNetArpG - 0x4C0000)  # "cat /proc/net/arp | grep %s | awk '{pri"...
00426CF0                addiu   $v1, $fp, 0x80+var_60
00426CF4                move    $a0, $v1          # s
00426CF8                move    $a1, $v0          # format
00426CFC                lw      $a2, 0x80+arg_0($fp)
00426D00                la      $v0, sprintf
00426D04                nop
00426D08                move    $t9, $v0
00426D0C                jalr    $t9 ; sprintf
00426D10                nop
00426D14                lw      $gp, 0x80+var_70($fp)
00426D18                addiu   $v0, $fp, 0x80+var_60
00426D1C                move    $a0, $v0          # command
00426D20                la      $v0, system
00426D24                nop
00426D28                move    $t9, $v0
00426D2C                jalr    $t9 ; system
00426D30                nop
00426D34                lw      $gp, 0x80+var_70($fp)
00426D38                addiu   $v0, $fp, 0x80+var_60
00426D3C                move    $a0, $v0          # command
00426D40                la      $v0, aAclServiceBloc  # "acl_service_block.rule_0"
00426D44                nop
00426D48                addiu   $a1, $v0, (aR_0 - 0x4C0000)  # "r"
00426D4C                la      $v0, popen
00426D50                nop
00426D54                move    $t9, $v0
00426D58                jalr    $t9 ; popen
```

```
Two: The key 'REMOTE_ADDR' pass to system:
```

```
00426C60                nop
00426C64                addiu   $v0, (aPingSW1DevNull - 0x4C0000)  # "ping %s -w 1 > /dev/null"
00426C68                addiu   $v1, $fp, 0x80+var_60
00426C6C                move    $a0, $v1          # s
00426C70                move    $a1, $v0          # format
00426C74                lw      $a2, 0x80+arg_0($fp)
00426C78                la      $v0, sprintf
00426C7C                nop
00426C80                move    $t9, $v0
00426C84                jalr    $t9 ; sprintf
00426C88                nop
00426C8C                lw      $gp, 0x80+var_70($fp)
00426C90                addiu   $v0, $fp, 0x80+var_60
00426C94                move    $a0, $v0          # command
00426C98                la      $v0, system
00426C9C                nop
00426CA0                move    $t9, $v0
00426CA4                jalr    $t9 ; system
```