

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 set_sta_enrollee_pin_wifi1 (or set_sta_enrollee_pin_wifi0) with the key 'wps_sta_enrollee_pin', allowing an authenticated user to run arbitrary commands on the device.

Detial

The bug in function: do_sta_enrollee_wifi, binary: www/cgi/ssi
The parameter 'wps_sta_enrollee_pin' pass to system

```
:00429CBC      la      $v0, aAclServiceBloc # "acl_service_block.rule_0"
:00429CC0      nop
:00429CC4      addiu   $a0, $v0, (aWpsStaEnrollee - 0x4C0000) # "wps_sta_enrollee_pin"
:00429CC8      la      $v0, getenv
:00429CCC      nop
:00429CD0      move   $t9, $v0
:00429CD4      jalr   $t9 ; getenv
:00429CD8      nop
00429F58      addiu   $v1, $v0, (aHostapdCliISWp_0 - 0x4C0000) # "hostapd_cli -i %s wps_pin any %s"
00429F5C      addiu   $a0, $fp, 0x130+var_10C # s
00429F60      addiu   $v0, $fp, 0x130+var_4C
00429F64      move   $a1, $v1 # format
00429F68      move   $a2, $v0
00429F6C      lw     $a3, 0x130+var_110($fp)
00429F70      la     $v0, sprintf
00429F74      nop
00429F78      move   $t9, $v0
00429F7C      jalr   $t9 ; sprintf
00429F80      nop
00429F84      lw     $gp, 0x130+var_120($fp)
00429F88      addiu   $v0, $fp, 0x130+var_10C
00429F8C      move   $a0, $v0 # command
00429F90      la     $v0, system
00429F94      nop
00429F98      move   $t9, $v0
00429F9C      jalr   $t9 ; system
```