TEW-827DRU

Firmware version

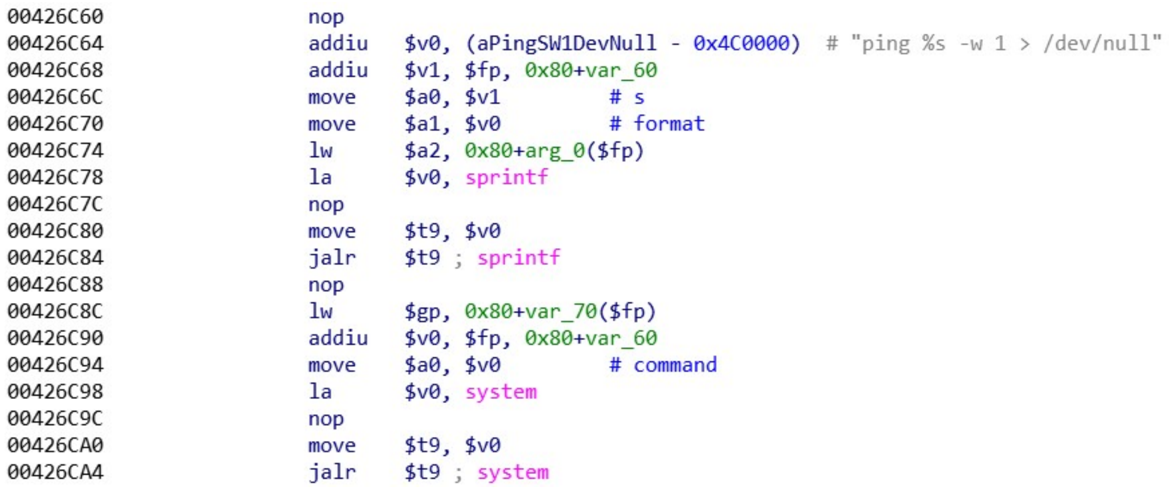
```
TEW-827DRU firmware: 2.06B04
```

Description

```
TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains a stack-
based buffer overflow in the ssi binary.
The overflow allows an authenticated user to execute arbitrary code by POSTing
to apply.cgi via the action wifi_captive_portal_login with a sufficiently long
key “REMOTE_ADDR”.
```

Detial

```
The bug in function: get_mac_from_ip_by_arptable, binary: www/cgi/ssi
The key 'REMOTE_ADDR' pass to sprintf:
```



```
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
```