

master

...

IoTirmware / Trendnet / TEW-827 / st_dev_reconnect_overflow.pdf

kuc001 add trendnet TEW-827DRU vulnerabilities

History

1 contributor

104 KB

...

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 st_dev_reconnect with a sufficiently long key "wan_type".

Detial

The bug in function: 0x42C30C, binary: www/cgi/ssi
The parameter 'wan_type' pass to sprintf

```
0042C348      addiu  $a0, $v0, (aWanType - 0x4C0000) # "wan_type"
0042C34C      la     $v0, getenv
0042C350      nop
0042C354      move  $t9, $v0
```