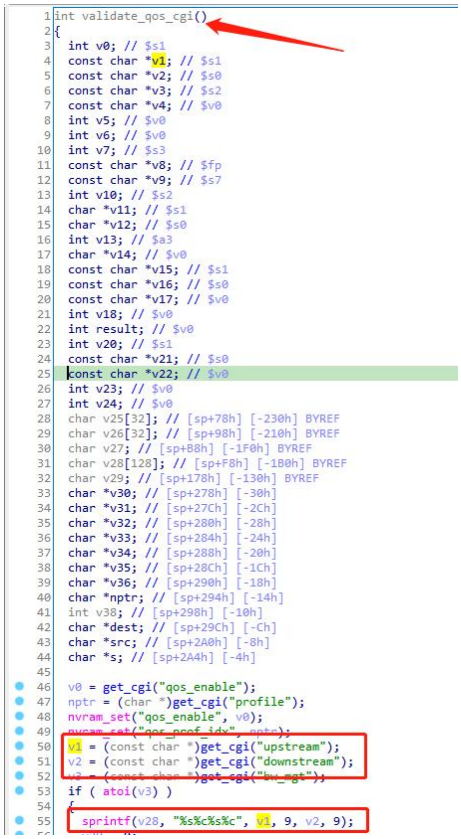
漏洞名称：belkin SKU F7D3302zh (f7d8302)存在缓冲区溢出漏洞

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



```
int validate_qos_cgi()
{
  int v0; // $s1
  const char *v1; // $s1
  const char *v2; // $s0
  const char *v3; // $s2
  const char *v4; // $v0
  int v5; // $v0
  int v6; // $v0
  int v7; // $s3
  const char *v8; // $fp
  const char *v9; // $s7
  int v10; // $s2
  char *v11; // $s1
  char *v12; // $s0
  int v13; // $a3
  char *v14; // $v0
  const char *v15; // $s1
  const char *v16; // $s0
  const char *v17; // $v0
  int v18; // $v0
  int result; // $v0
  int v20; // $s1
  const char *v21; // $s0
  const char *v22; // $v0
  int v23; // $v0
  int v24; // $v0
  char v25[32]; // [sp+78h] [-230h] BYREF
  char v26[32]; // [sp+98h] [-210h] BYREF
  char v27; // [sp+B8h] [-1F0h] BYREF
  char v28[128]; // [sp+F8h] [-1B0h] BYREF
  char v29; // [sp+178h] [-130h] BYREF
  char *v30; // [sp+278h] [-30h]
  char *v31; // [sp+27Ch] [-2Ch]
  char *v32; // [sp+280h] [-28h]
  char *v33; // [sp+284h] [-24h]
  char *v34; // [sp+288h] [-20h]
  char *v35; // [sp+28Ch] [-1Ch]
  char *v36; // [sp+290h] [-18h]
  char *nptr; // [sp+294h] [-14h]
  int v38; // [sp+298h] [-10h]
  char *dest; // [sp+29Ch] [-Ch]
  char *src; // [sp+2A0h] [-8h]
  char *s; // [sp+2A4h] [-4h]

  v0 = get_cgi("qos_enable");
  nptr = (char *)get_cgi("profile");
  nvram_set("qos_enable", v0);
  nvram_set("qos_prof_idx", nptr);
  v1 = (const char *)get_cgi("upstream");
  v2 = (const char *)get_cgi("downstream");
  v3 = (const char *)get_cgi("bw_mgt");
  if ( atoi(v3) )
  {
    sprintf(v28, "%s%c%s%c", v1, 9, v2, 9);
```

漏洞复现：

使用 FirmAe 仿真固件

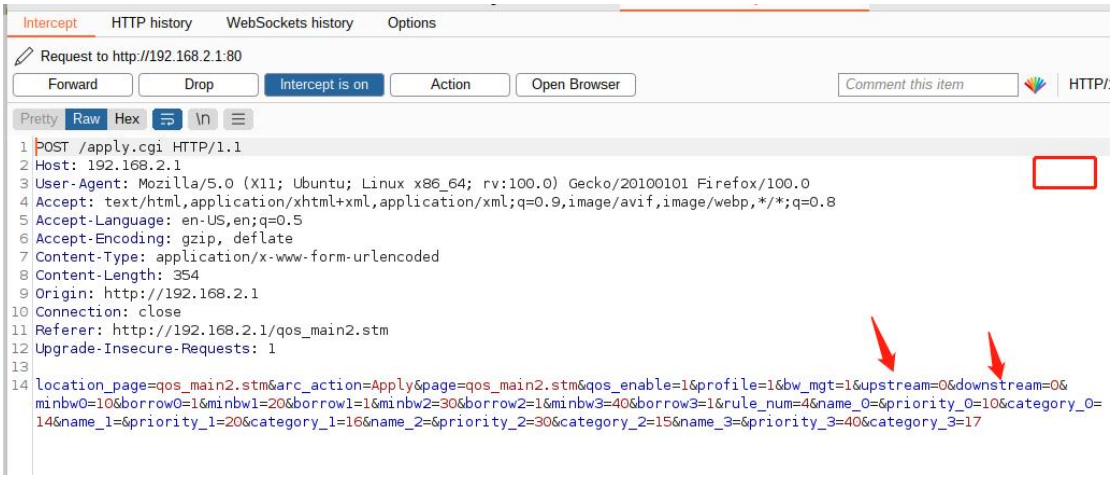
```
FirmAE$ sudo ./run.sh -d belkin ./firmwares/F7D4302-8302_WW_1
.00.28.bin
[sudo] password for iot:
[*] ./firmwares/F7D4302-8302_WW_1.00.28.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] ./firmwares/F7D4302-8302_WW_1.00.28.bin already succeed emulation!!!

[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
7
```

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

将 upstream 或 downstream 的值更改为超长字符串，发送



此时 web 服务器已经崩溃，无法访问