Sri Lanka Institute of Information Technology

Arbitrary File Read Vulnerability – A Case Study

IE3022 – Mobile Security

Assignment - 1

Submitted by	Registration Number
M. Thushitharan	IT19983370

Submission Date:

18/06/2022

Table of contents

1. Abstract

This case study is to analyze the Arbitrary File Reading Vulnerability and exploit that vulnerability using ES File Explorer application's vulnerable version in android mobile. This leads to read the arbitrary files on the android system through the application. To explore the vulnerability details, I have clarified about arbitrary files, TCP Ports, Metasploit and the es file explorer application. And I mentioned attack virtual environment setup for exploit this vulnerability in controlled environment. And finally, I mentioned the mitigation methods for this vulnerability as well. This study was analyzed via the search for the referrals, research papers and reading materials from roaming the web.

2. Introduction

This Case study will explain about 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.

3. Executive Summary

3.1. Scope of the Test

The scope of this case study is analyze Arbitrary File Read Vulnerability and Exploit this vulnerability with the use of an android application called Es File Explorer. For this exploitation I selected CVE-2019-6447 patch.

3.2. Scope of Impact

Vulnerability Affected Versions of ES File Explorer: **v4.1.9.7.4(except earlier and after versions)**

4. Explanation

4.1. What is an Arbitrary File?

An arbitrary file is any file on a specific server or system. Basically, the arbitrary file is a file that allows you to modify everything on a system. For example, if you got access to a particular website part of a shared server and you manage to root it, the files from the "box" are arbitrary - those on the site itself are not. This vulnerability also leads the applications to do path traversal.

4.2. What is CVE-2019-6447?

CVE-2019-6447 is an Arbitrary File Reading vulnerability which is found on ES File Explorer File Manager application through 4.1.9.7.4 for Android. This 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 through HTTP. Simply if you opened the app at least once, anyone connected to the same local Wi-Fi network can remotely handle any file from your phone.

CVE Base score of this Vulnerability is **8.1**

4.3. What is ES File Explorer?

ES File Explorer is a file manager/explorer designed by ES Global, a subsidiary of DO Global, for Android devices. It includes features like cloud storage integration, file transfer from Android to Windows via FTP or LAN, and a root browser. As per the google play store statistic, ES File Explorer that potentially expose hundreds of million Android installs. Once this application was removed from the Google Play Store for committing click fraud.

4.4. What is TCP Port?

Ports are numbered and used as global standards to identify specific processes or types of network services. Much like before shipping something to a foreign country, you'd agree where you'd be shipping out of and where you'd have it arriving, TCP ports allow for standardized communication between devices.

4.5. What is Metasploit?

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

5. Exploitation

5.1. Virtual Environment

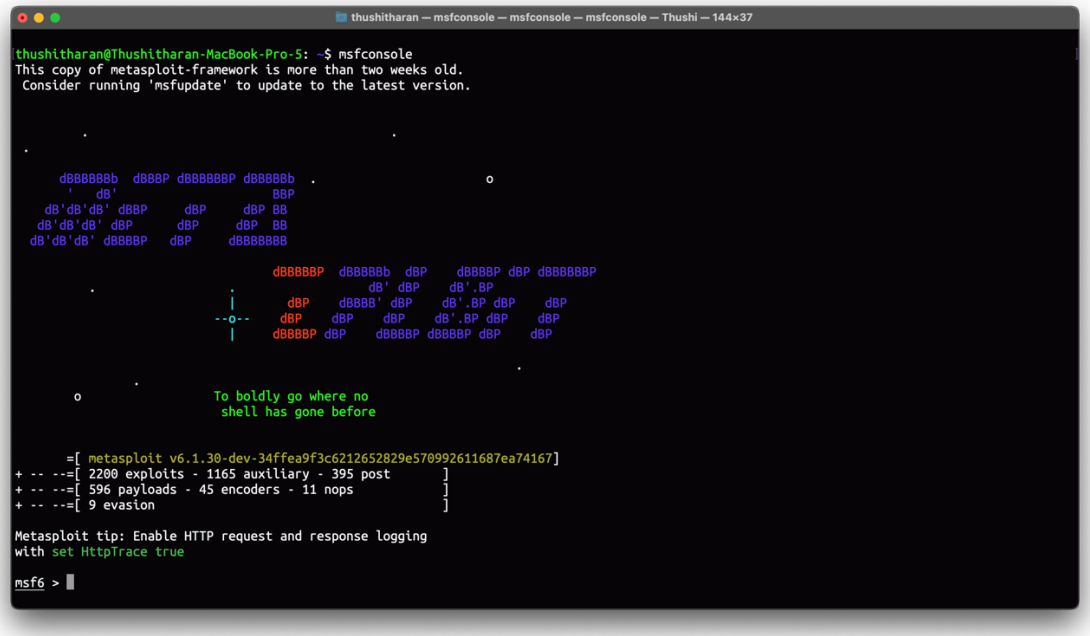
I have done this exploitation in Mac Operating system. I installed vulnerable ES File Explorer application (version 4.1.9.7.4) in an android mobile. Then I connected the computer and the mobile in a same Wi-Fi network. I used Network Radar software for scan the connected networks in my local network.

5.2. Local Network

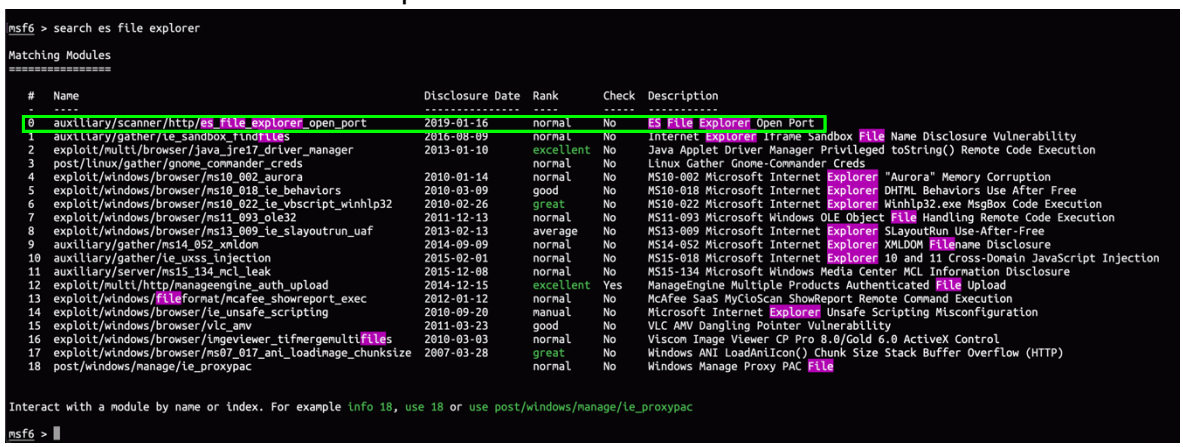
There are two types of messages: Requests sent by clients and responses by the server. In HTTP messages the textual information is encoded in ascii. In earlier versions like HTTP/1.1 messages were sent across the connection openly. In latest versions, HTTP/2.0, the human readable message is divided into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

5.3. Exploitation Steps

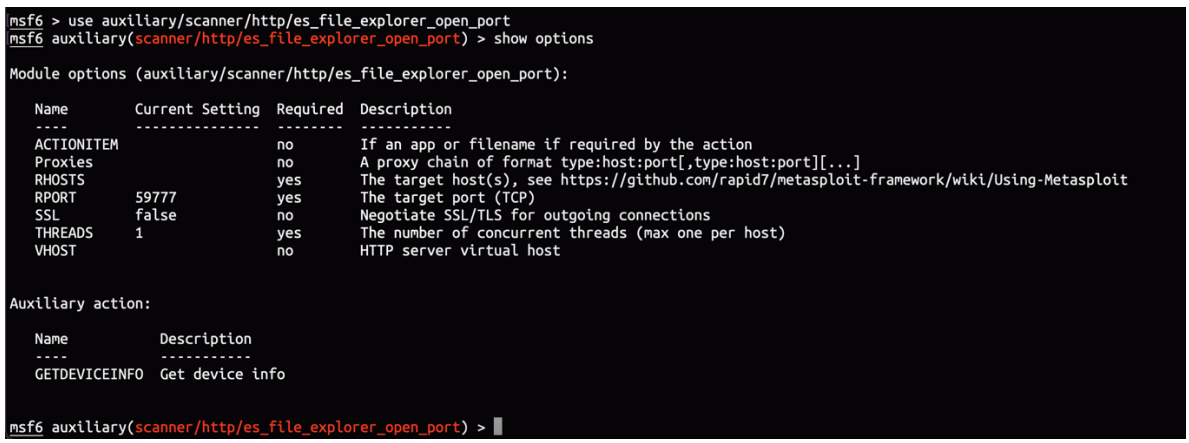
1. I opened Metasploit console in the Mac OS Terminal



2. Then I searched for the es file explorer module and the exploit for module was found in first line in the Metasploit database.

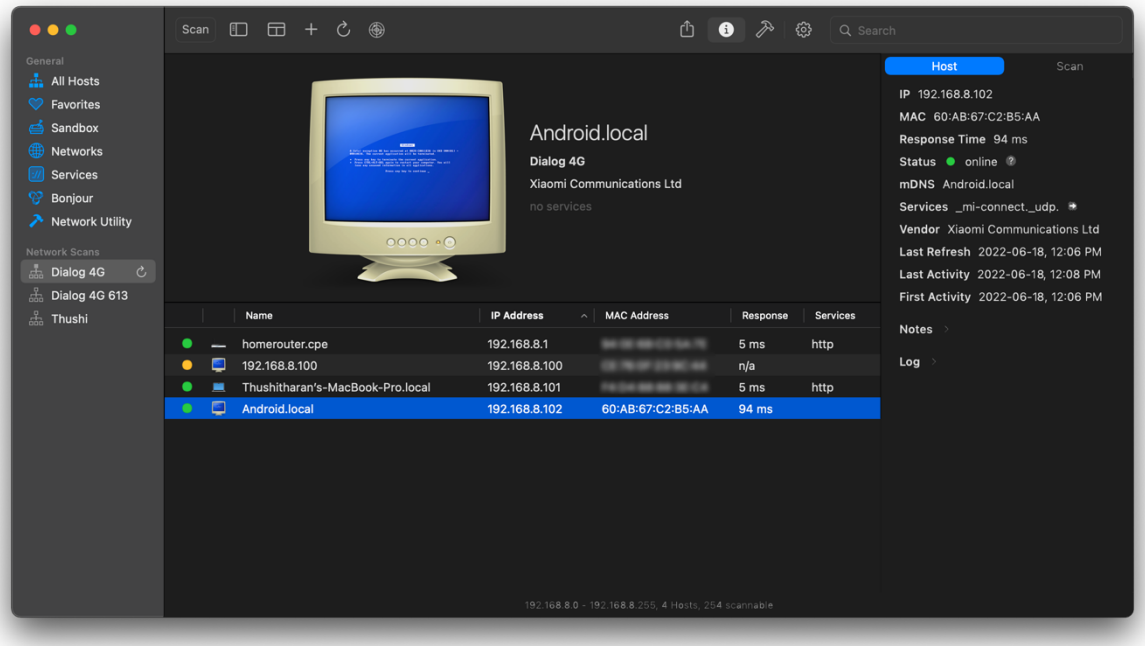


3. Then I selected the module called auxiliary/scanner/http/es_file_explorer_open_port and view the options which needed to set.

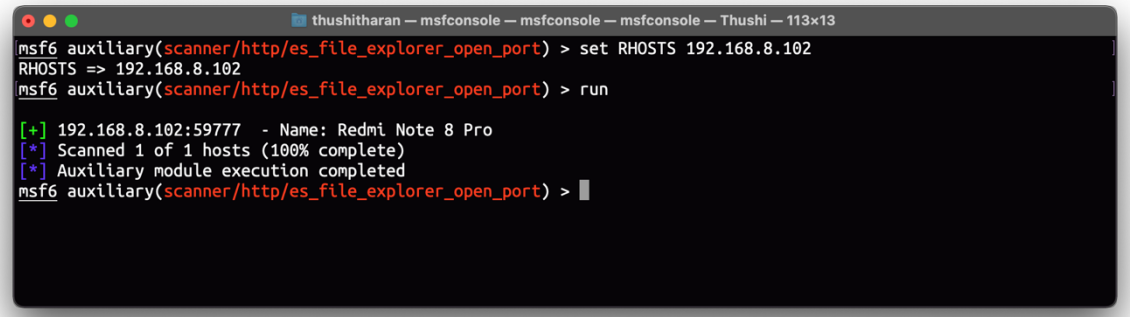


There is TCP port 59777 has already set for this exploit module.

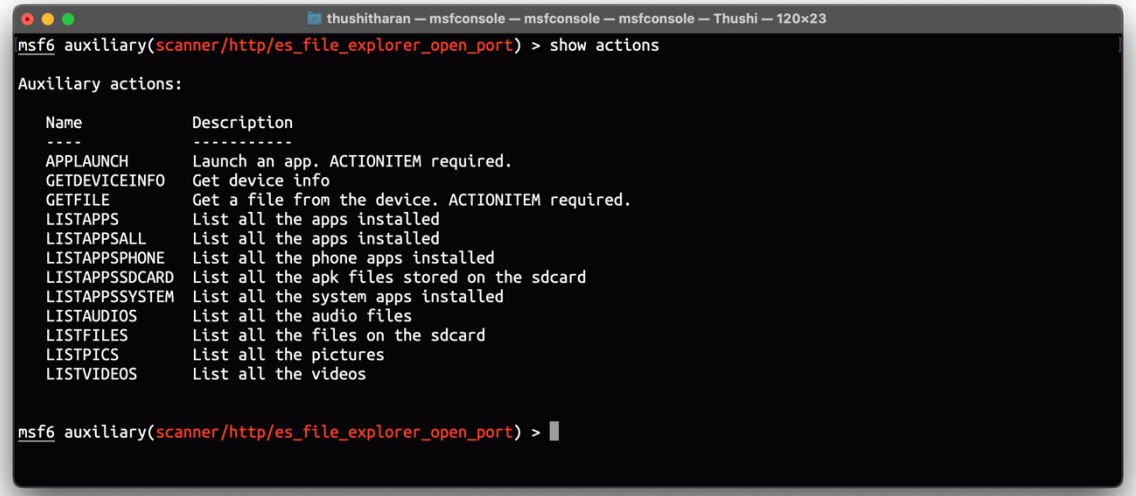
4. Next, I needed to set RHOSTS option. So, I connected an android mobile in my same network and found its local network IP address using Network Radar Software which I installed in my MacOS.



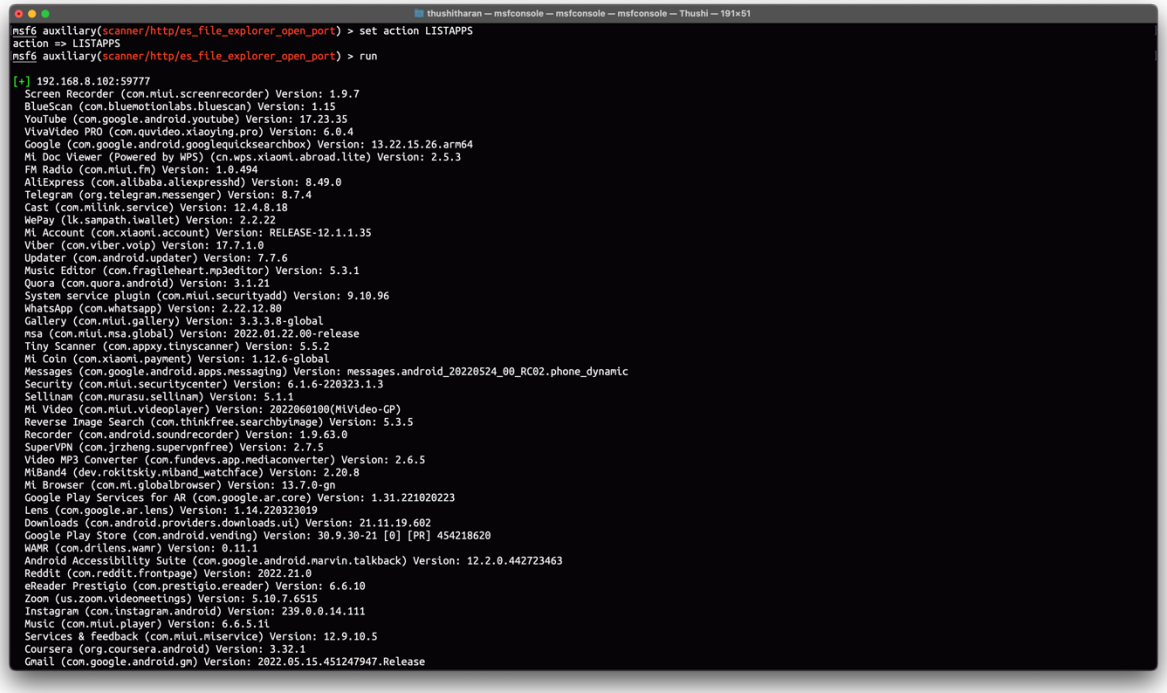
5. Then I set the found IP address to the RHOSTS options and run the module.



6. Now I ran show actions command to check available actions that we can perform on the device through this exploitation.



7. Then I changed the action to LISTAPPS to list out the applications from the connected mobile. Then I run it. BOOM!!! It's working, It is showing the installed applications in the connected mobile.



6. Mitigation

This vulnerability can be eliminated by updating the latest version of the ES File Explorer application. Current latest version is 4.2.9.2.1

7. References

1. https://securityaffairs.co/wordpress/80057/hacking/es-file-explorer-flaws.html
2. https://www.javatpoint.com/tcp-port
3. https://en.wikipedia.org/wiki/ES_File_Explorer
4. https://www.varonis.com/blog/what-is-metasploit
5. https://medium.com/@knownsec404team/analysis-of-es-file-explorer-security-vulnerability-cve-2019-6447-7f34407ed566
6. https://github.com/fs0c131y/ESFileExplorerOpenPortVuln
7. https://portswigger.net/web-security/file-path-traversal#:~:text=Directory%20traversal%20(also%20known%20as,and%20sensitive%20operating%20system%20files.
8. https://www.youtube.com/watch?v=5bit5PF6arg
9. https://www.researchgate.net/publication/349768070_Exploiting_Android_Vulnerability_in_ES_File_Explorer_CVE-2019-6447_Paper
10. https://techcrunch.com/2019/01/16/android-app-es-file-explorer-expose-data/