Android Stagefright

Logan Bair

Department of Computer & Information Sciences   
College of Science & Mathematics   
Towson University

Lbair89@gmail.com

Mary Snyder

Department of Computer & Information Sciences  
College of Science & Mathematics  
Towson University

msnyde8@students.towson.edu

**ABSTRACT**

In this paper, we describe our approach for implementing the known exploit for the Android operating system (OS) Stagefright vulnerability on numerous releases of the Android OS ranging from versions 4.0-5.1.

**Categories and Subject Descriptors**

K.6.5 [Management of Computing Information Systems]: Security and Protection

**Keywords**

Security; Stagefright; Zimperium Research Labs (zLABS); Android Open Source Project (AOSP); SMS; MMS

# INTRODUCTION

Security researchers at Zimperium Research Labs (zLABS) recently discovered an Android OS vulnerability. To exploit this vulnerability, the attacker merely needs access to the phone’s mobile number and can gain remote code execution privileges. The Android Open Source Project (AOSP) contains a media library named Stagefright at its core which is responsible for processing of all multimedia files (videos, audio, and documents).

The vulnerability found in Stagefright is especially dangerous because it requires no interaction from the device user. Multimedia files are pre-processed by Stagefright as they are received to insure they are ready for use/viewing when the device user needs them. This pre-processing causes any malicious code embedded in the multimedia file to be executed even before the multimedia file is accessed by the device user.

<Write more here?>

# BACKGROUND ON STAGEFRIGHT

## Normal or Body Text

The VP of Platform Research and Exploitation at Zimperium zLabs, Joshua J. Drake discovered the vulnerability after delving into the inner workings of the Android OS.

When dealing with multimedia files time is of the essence and speed of processing is a high priority. As such, the Stagefright library was not written in Java or a similar more memory-safe language, but instead was based in C++, which is more apt to suffer from memory corruption.

Please use a 9-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

## Potential Disaster

The Stagefright vulnerability is said to effect 95% of all Android devices, an estimated 950 million.[[1]](#footnote-1) Ther

title (Helvetica 18-point bold), authors' names (Helvetica 12-point) and affiliations (Helvetica 10-point) run across the full width of the page – one column wide. We also recommend phone number (Helvetica 10-point) and e-mail address (Helvetica 12-point). See the top of this page for three addresses. If only one address is needed, center all address text. For two addresses, use two centered tabs, and so on. For more than three authors, you may have to improvise.[[2]](#footnote-2)

## First Page Copyright Notice

Please leave 3.81 cm (1.5") of blank text box at the bottom of the left column of the first page for the copyright notice.

## Subsequent Pages

For pages other than the first page, start at the top of the page, and continue in double-column format. The two columns on the last page should be as close to equal length as possible.

Table 1. Table captions should be placed above the table

|  |  |  |  |
| --- | --- | --- | --- |
| **Graphics** | **Top** | **In-between** | **Bottom** |
| Tables | End | Last | First |
| Figures | Good | Similar | Very well |

## References and Citations

Footnotes should be Times New Roman 9-point, and justified to the full width of the column.

Use the “ACM Reference format” for references – that is, a numbered list at the end of the article, ordered alphabetically and formatted accordingly. See examples of some typical reference types, in the new “ACM Reference format”, at the end of this document. Within this template, use the style named *references* for the text. Acceptable abbreviations, for journal names, can be found here: <http://library.caltech.edu/reference/abbreviations/>. Word may try to automatically ‘underline’ hotlinks in your references, the correct style is NO underlining.

The references are also in 9 pt., but that section (see Section 7) is ragged right. References should be published materials accessible to the public. Internal technical reports may be cited only if they are easily accessible (i.e. you can give the address to obtain the report within your citation) and may be obtained by any reader. Proprietary information may not be cited. Private communications should be acknowledged, not referenced (e.g., “[Robertson, personal communication]”).

## Page Numbering, Headers and Footers

Do not include headers, footers or page numbers in your submission. These will be added when the publications are assembled.

# BACKGROUND ON STAGEFRIGHT

All material on each page should fit within a rectangle of 18 × 23.5 cm (7" × 9.25"), centered on the page, beginning 1.9 cm (0.75") from the top of the page and ending with 2.54 cm (1") from the bottom. The right and left margins should be 1.9 cm (.75"). The text should be in two 8.45 cm (3.33") columns with a .83 cm (.33") gutter.

# FIGURES/CAPTIONS

Place Tables/Figures/Images in text as close to the reference as possible (see Figure 1). It may extend across both columns to a maximum width of 17.78 cm (7”).

Captions should be Times New Roman 9-point bold. They should be numbered (e.g., “Table 1” or “Figure 2”), please note that the word for Table and Figure are spelled out. Figure’s captions should be centered beneath the image or picture, and Table captions should be centered above the table body.

# TECHNIQUES FOR REPRODUCTION

<Write text here>.



Figure 1. Insert caption to place caption below figure.

.

## Environment

The heading of subsections should be in Times New Roman 12-point bold with only the initial letters capitalized. (Note: For subsections and subsubsections, a word like *the* or *a* is not capitalized unless it is the first word of the header.)

### Android x86 OS

We initially planned to use the Android x86 version of the OS for replicating the Stagefright exploit; however we were unable to find a way to emulate sending of text messages, specifically MMS messages with this version of the OS. Since MMS is one of the best and most likely way this exploit would be delivered to the public, we decided to find an environment that would allow us to deliver the exploit in this manner.

### Android Studio

After our issues with the Android x86 OS we tried Android Studio to spin up virtual instance of Android on PC. Android Studio allows the user to install and load any version of the Android OS on many different phone emulators. According to our research, the Android Emulator version allows for sending of SMS text messages through the command “sms send <senderPhoneNum> <textMsgBody>”.

Unfortunately after playing with the Android Emulator we discovered it would not meet our needs. While it is able to send SMS text messages, it is unable to send MMS messages. Since multimedia files are transmitted as MMS messages, not SMS messages, we would have to find another way to transmit the MMS message in this tool.

Before moving from Android Studio to yet another tool, we also looked at the possibility of using the Andoid app Google Hangouts to transmit the malicious MMS. Google Hangouts comes standard on the Android OS and allow for SMS/MMS integration; however, even our attempts using Google Hangouts in Android Studio were unsuccessful and we were forced to find another way to deliver the exploit to the device.

### VMs and Physical Devices

We finally employed the use of Genymotion VMs (versions 4.1-4.4 as well as less vulnerable versions 4.4-5.1), VMs in the Android SDK emulator (again on vulnerable versions 4.1-4.4 as well as 4.4-5.1), and even a physical Nexus 7 tablet running 4.1. After more research we discovered our issues with using Google Hangouts was due their disabling of MP4 messages, which was the type of file we were using as an exploit package. However, Zimperium zLabs also divulged the phone was vulnerable in whatever way the file could get onto the system, so we were able to deliver the exploit package through other means (methods discussed previously in <>).

#### Subsubsections

The heading for subsubsections should be in Times New Roman 11-point italic with initial letters capitalized.

#### Subsubsections

The heading for subsubsections should be in Times New Roman 11-point italic with initial letters capitalized.

# <>

Blah blah blah de blah.

# CONCLUSION

Blah blah blah de blah.

# ACKNOWLEDGMENTS

Our thanks to ACM SIGCHI for allowing us to modify templates they had developed. Blah blah blah de blah.

# REFERENCES

1. Zimperium Mobile Security Blog. “Experts Found A Unicorn In The Heart Of Android” N.p., https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/ Web. 05 Nov. 2015.
2. YouTube: Blackhat “Stagefright: Scary Code in the Heart of Android” https://www.youtube.com/watch?v=71YP65UANP0 Web. Nov. 2015
3. Exploit Database. “Android Stagefright – Remote Code Execution” N.p., https://www.exploit-db.com/exploits/38124/ Web. 05 Nov. 2015.
4. Hacker 9: The Unruly Security Channel. “Hacking any android smartphone using ‘Stagefright’ vulnerability” N.p., http://www.hacker9.com/hack-android-smartphone-vulnerability.html Web. 05 Nov. 2015.
5. The Hacker News: Security in a serious way. “How to Hack Millions of Android Phones Using Stagefright Bug, Without Sending MMS” N.p., http://thehackernews.com/2015/07/how-to-hack-android-phone.html Web. 05 Nov. 2015.
6. Exploit Database. “Android libstagefright – Integer Overflow Remote Code Execusion” N.p., https://www.exploit-db.com/exploits/38226/ Web. 05 Nov. 2015.
7. How-To Geek. “How to Install Android in VirtualBox” N.p., http://www.howtogeek.com/164570/how-to-install-android-in-virtualbox/ Web. 05 Nov. 2015.
8. Developer.android.com. “Android Studio Overview” N.p., http://developer.android.com/tools/studio/index.html Web. 05 Nov. 2015.
9. Developer.android.com. “Using the Emulator” N.p., http://developer.android.com/tools/devices/emulator.html Web. 05 Nov. 2015.
10. Genymotion. N.p., https://www.genymotion.com/#!/ Web. 05 Nov. 2015.

Columns on Last Page Should Be Made As Close As Possible to Equal Length

1. If necessary, you may place some address information in a footnote, or in a named section at the end of your paper. [↑](#footnote-ref-1)
2. If necessary, you may place some address information in a footnote, or in a named section at the end of your paper. [↑](#footnote-ref-2)