MWR LABS

Security Advisory

Android Premium SMS Warning Manipulation

20/09/2016

Software	Android Open Source Project (AOSP)
Affected Versions	6.0.1 and earlier
CVE Reference	CVE-2016-3883
Author	Rob Miller
Severity	Medium
Vendor	Google
Vendor Response	Patch Released

Description:

The Android Telephony API is used by applications to handle SMS and MMS sending and receiving. To restrict applications from sending premium rate SMS messages without user consent, the Telephony API will produce a warning dialog explaining the intention of the sending application and that the action will cost the user money. The user must then tap “Send” for the SMS to be sent. This restriction was put in place as many instances of malware would use premium rate SMS messages as a way of profiteering by sending messages to numbers owned by the malware’s authors.

It was found that the warning message used the “app_name” string from the application itself to form part of the message. This message would then have all HTML tags rendered using the Html.fromHtml() function. An attacker would therefore be able to include HTML tags in their application name to manipulate this warning message, potentially tricking a user into sending the premium rate SMS messages.

Impact:

Malware installed on an Android device could include HTML tags in its application name. Upon sending a premium rate SMS message, the user would not receive the legitimate warning, but rather one controlled by the malware. This may lead to users sending the messages and incurring financial loss.

Cause:

The Telephony API is used by applications to manage sending and receiving SMS and MMS messages. To stop applications automatically sending messages that would cost the user money, the user is prompted as to whether or not they want the app to send the message. The message includes the sending application's name.

As the application's name is put in to the warning message, and then rendered as HTML, a malicious app could misuse this feature to change the text in the warning message by including HTML tags within its application name. This can change the warning message to show any text that the malicious app chooses to show.

Solution:

Google have released a security update through an over-the-air (OTA) update as part of its Android Security Bulletin Monthly Release process. Please refer to the Android Security Bulletin – September 2016: https://source.android.com/security/bulletin/2016-09-01.html

Technical details:

The Telephony API checks whether SMS messages sent by applications are destined for premium rate numbers by checking against known short code formats. If the SMS matches this format then the SMSDispatcher's handleConfirmShortCode() is called, passing details of the application making the request.

The application's name is retrieved and stored in the appLabel variable:

```
CharSequence appLabel = getAppLabel(tracker.mAppInfo.packageName);
```

The sms_short_code_confirm_message string is used as a template for the warning message. Its raw format is as follows:

```
&lt;b&gt;<xliff:g id="APP_NAME">%1$s</xliff:g>&lt;/b&gt; would like to send a message to
&lt;b&gt;<xliff:g id="DEST_ADDRESS">%2$s</xliff:g>&lt;/b&gt;.
```

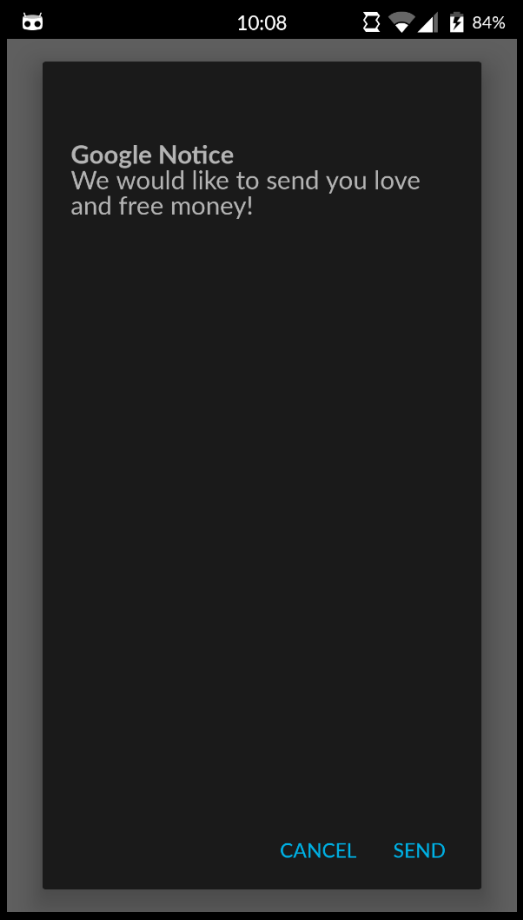
The application name is then added to the message string, and then rendered as HTML:

```
Spanned messageText = Html.fromHtml(r.getString(R.string.sms_short_code_confirm_message,
appLabel, tracker.mDestAddress));
```

Therefore if the application was to have the following entry in its values.xml file:

```
<string name="app_name">&lt;LegitApp>
                                    &lt;br>Google Notice &lt;/b> &lt;br>We would like to send
you love and free money!&lt;br/>









                        </string>
```

Then when the application sent a SMS to a premium rate number, the following error message would be displayed:



Detailed Timeline

Date	Summary
2016-05-03	Issue raised on the AOSP Issue Tracker (Issue #208949)
2016-05-10	Issue marked as moderate severity by Google security team
2016-09-01	Android Security Bulletin (September 2016) Published
2016-09-20	Advisory released