950 Million Android Phones Vulnerable to Hacking

July 28, 2015 â€“ If you havenâ€™t been paying attention to the news this morning, you may have missed the latest hacking vulnerability. This one involved virtually every single cell phone powered by Android worldwide. The most frightening thing about this is that the only thing a hacker needs to know to gain access to everything on your phone is your phone number. But there are some things you can do to protect yourself. Here is what you need to know.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
  var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
  po.src = 'https://apis.google.com/js/plusone.js';
  var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

What is the hack called?

The hack is being referred to as â€œStagefrightâ€•. The name is based on Googleâ€™s Stagefright engine which is used to pla back videos on Android phones.

What does the hack do?

Once triggered, the hacker can gain access to all of the information on your cell phone including credit card information and stored files. The hacker can also use your phone to record video, take pictures and record sound without your knowledge.

How does it work?

The hack is actually vulnerability in Android phones. A hacker can send a multimedia message (MMS) to your phone that plays a video. (Most people refer to MMS and SMS messages the same way; as â€œtextâ€• messages.) Depending upon the settings of the program you use for MMS messages, the hack can be triggered as soon as you receive the messageâ€¦ meaning that you donâ€™t even have to open the message up.

Which phones are vulnerable?

Any cell phone running Android 2.2 and above. That means virtually every single Android phone sold in the past five years. It affects approximately 950 million phones that are currently in use.

Is there a security patch available?

Sort of. Google has already released a security patch but it isnâ€™t something that you can download and install yourself. It has been provided to all cell phone carriers, and they tend to be very slow in rolling out updates to their users. Anyone having a rooted phone (if you donâ€™t know what that means then you donâ€™t have one) running Cyanogen Mod should be able to get the update very soon as the developers have announced that the patch will be included in all releases from now on. But if you are running a stock Android device that you received from your cell phone carrier, you are going to have to wait.

What can I do in the meantime to protect myself?

Until your carrier releases and update, you need to disable autoretrieval of MMS messages in your texting app. twiloBlog has an easy to follow explanation of how to go about this. This is especially important for anyone using Google Hangouts to process their text messages. Hangouts processes messages before the user actually reads them. This means that the user doesnâ€™t even have to read the message in order for the hack to take place. Hangouts is the default messaging app for millions of users.

How worried do I need to be?

The Stagefright vulnerability is very bad. It has the potential to be the largest vulnerability ever detected in Android. But with that said, androidcentral.com is pointing out that it has been available to hackers for the past five years and there hasnâ€™t been a single reported incident in that time. Given the publicity Stagefright is getting this week though, that is likely to change. The bottom line here is that you need to be proactive and take the steps required to disable automatic processing of MMS messages right away. Not doing so could lead to fraud, invasions of privacy and identity theft.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS