Workplace Service

First Cut
Number: 2013-FC10
July 30, 2013

Aragon Research

Author: Lou Latham

Topic: Mobile

Issue: What are the trends impacting mobile computing?

Security Bug Could Affect Nearly Every Android Device

***Summary**: A security research firm has found a flaw in the Android operating system that makes nearly a billion phones and tablets vulnerable to malware intrusion. The vulnerability has already been exploited. Google has created a fix, but many devices may never get it.*

Event: In February, 2013 security research firm BlueBox Security notified Google of a security vulnerability in the Android mobile operating system code. Google later released a fix to carriers and manufacturers. In July 2013, Symantec discovered multiple exploits of this flaw.

Analysis

Bluebox discovered a coding error in Android that would allow a hacker to hide malicious code in an Android app without tripping the internal alarm that is supposed to detect such changes. Bluebox says the flaw (the “Master Key” vulnerability) makes it possible to alter an Android app without changing its cryptographic signature, which verifies that the app is legitimate. This tricks Android into reporting that an app has not been tampered with, even if it has been.

Bluebox notified Google in February 2013, and Google issued a corrective patch in March. Many phones with firmware installed after April 2013 will have the fix; the first one we know of is the Samsung Galaxy S4. However, nearly a billion older phones are still vulnerable until their firmware is updated.

On July 23, 2013, Symantec discovered the first known exploit of this flaw, in an Android app installer (.apk) file from a third-party app store. The payload is a Trojan called Android.Skullkey that takes control of the phone, sending text messages and stealing user data. There is no evidence that the exploit has done significant damage, but it is clear that the vulnerability has been successfully analyzed.

Because it doesn’t distribute Android updates directly to users (except for a small number of Nexus devices), Google can’t fix this alone. The fix is implemented in the device firmware, so each manufacturer has to build a solution for each model. Carriers also have to participate in delivering the update to customers. This means the availability of fixes for different devices will vary widely. Some devices may never be fixed.

Bluebox has distributed a diagnostic tool that will tell you whether or not your device has the flaw and whether any apps on your device contain the code to exploit it. The diagnostic is in the Google Play store, called “Bluebox Security Scanner.” Google has also updated the security filter in the Play store itself, so the store will not download an app that exploits the flaw. The Amazon and GetJar stores are now similarly protected.

At some point, Google will release one or more versions of Android with the fix built in, and we’ll publish the version numbers when we learn them. That doesn’t mean that any particular version will run on any particular phone, though. Android provisioning decisions are divided among Google, the device manufacturers and the wireless carriers, and governed by many factors.

There's no reason to panic about this. There are always security holes in operating systems. This isn't the last one; there will never be a last one. However, we shouldn't be complacent, either. Most phones run Android, so it's a tempting target. While Symantec rates the damage potential of the current exploit as moderate, the next payload could be anything. Mobile devices affect our lives in many more ways than PCs do. An attack could blow out your phone bill with roaming charges or hidden calls; it could spoof your GPS and get you lost, or disable the phone in a variety of ways. If you BYOD, it could also get into your corporate network and cause more serious mischief.

Users as well as enterprises benefit from robust enterprise mobile management in the workplace. Aragon has an extensive library of research on EMM (including, for paid subscribers, the recent *Aragon Research Globe for Enterprise Mobile Management Software, 2013*).

Aragon Advisory

- Enterprises evaluating mobile security products should ensure that all their candidate solutions include screening for this flaw. The same filter that protects the Google store can protect an enterprise app store.
- Users should set their devices to reject third-party sideloads, which can occur without their knowledge. Download apps only from stores that are protected: currently these are Google, Amazon and GetJar.
- Users should download and run the Bluebox Security Scanner from the Google Play store, and ensure that other scanning apps will scan for this flaw.
- Users shopping for an Android device should know which models have the fix and which do not. Most devices built after mid-2013 should be safe, but not all available devices were recently built. Heavily discounted older phones may not be safe.
- Enterprises with EMM capability should ensure that Android devices within their domains are set to reject app downloads from unauthorized sources, and push available patches to any device that will take them. They should also consider offering subsidies to replace devices too old to be patched.

Bottom Line

Mobile device security remains a critical area to monitor. Carriers need to be more vigilant with upgrades to devices, when it comes to major security flaws. Enterprises need to educate their users about Android settings and how they affect security, and make use of EMM software, which can improve security through advanced device management.

Related Aragon Research

- Mobile Upgrades – Apple iOS and Microsoft Windows Phone Trump Android
- Facebook Home: Good for Users and Android; Bad for Google and Business
- Firefox Mobile OS Faces Huge Enterprise Hurdles
- Apple's Focus on the iPad Gave Samsung an Opening