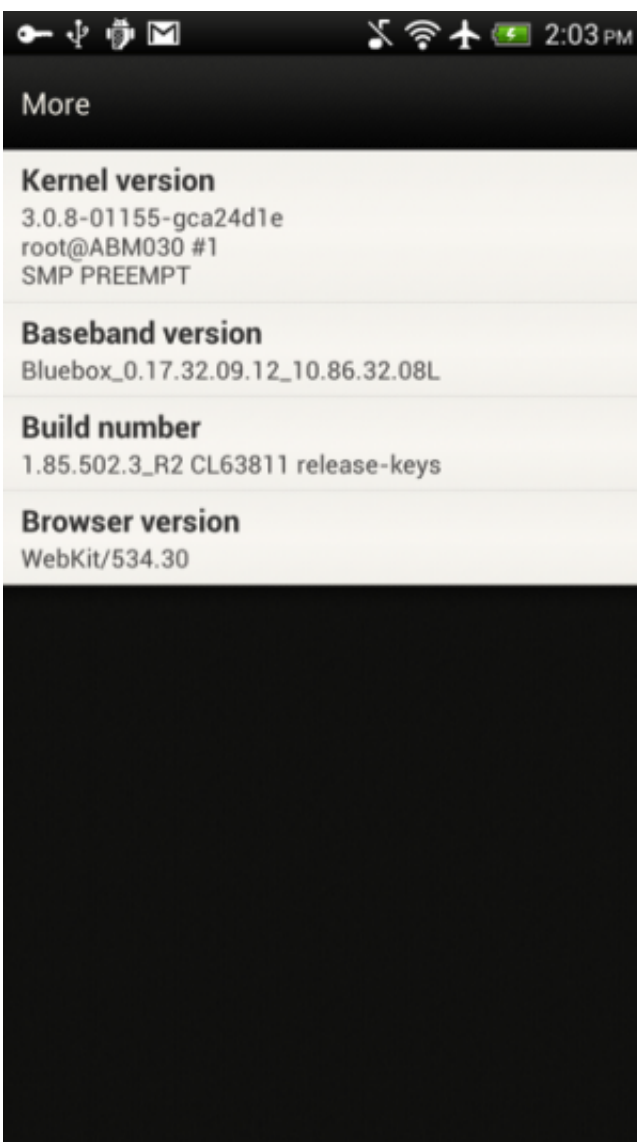# Bluebox Security reveals Android vulnerability in run up to Blackhat convention

July 4 2013, by Bob Yirka

Screenshot of HTC Phone After Exploit

(Phys.org) —Mobile security startup Bluebox Security has revealed via a post on its website a vulnerability in smartphones running the Android operating system. The vulnerability, they say could allow hackers to modify code in apps running on a phone without breaking the app's cryptographic signature.

Normally when an app is downloaded from a reliable source, it comes with something called the Android Application Package File (APK). The purpose of the file is to allow the app to prove that it's not been modified since being installed—a sign that it's been hacked and changed. A check is made every time the app is run. To make it more difficult for hackers to modify existing apps, the APK is given a cryptographic signature. Now Bluebox is reporting that they've found a way to modify existing apps on a smartphone, without disturbing the cryptographic signature. Worse, they say, the vulnerability goes all the way back to Android 1.6, which was released nearly four years ago. That they say, means that 900 million devices are currently at risk.

Modification of an app allows a hacker to cause the app to do things the user is not aware of, such as access data. One of the most serious scenarios, Bluebox says, is if an app made by the manufacturer of a phone is changed. Such apps, they note, generally have access to phone functionality in addition to services such as text messages. That means a modified app could be made to control the phone's camera, for example, or to place calls.

Bluebox isn't revealing exactly how a hacker might take advantage of the vulnerability—that would be inviting trouble, of course. They do say that they notified Google of what they'd found back in February, and that presumably the tech giant is working on a solution. In the meantime, they suggest phone users abstain from downloading apps from risky third

party sites. They also strongly encourage enterprise managers to encourage all users of a given system to update their devices as soon as a fix becomes available. The company is also promising to reveal more about the nature of the vulnerability at this year's Black Hat USA 2013 conference.

© 2013 Phys.org