



## **Caveat emptor (Buyer beware) with Android devices**

In early October we posted the article [Peeking Behind the Curtain on Android vs. iOS Decisions](#). That article exposed that, while many Android devices are way cheaper than an equivalent iOS device, that comes at the expense of little to no OS upgrade path.



To verify this I did go ahead and buy a cheap Android tablet, a refurbished Hisense Sero 7 Pro. The research I did before purchasing indicated that there were some user community hacks to take the device from the stock Android 4.2 JellyBean to at least Android 4.4 KitKat. (There was an article on how to go to Android 5.x, but that post was withdrawn by the time I received my unit. Go figure.)

Why is this important to you? Security. There are some serious security flaws that are identified with each release of the Android OS. That is true of iOS as well. The difference is

that iOS devices have a longer upgrade life, and an EASIER upgrade process, than corresponding Android devices. The exception to this are devices made by Google, but those devices are typically equivalent in price to a corresponding iOS device.

Don't believe the seriousness? Here is a quote from a recent article by Graham Cluley, whom we often quote.

"[M]y advice is that if you have a vulnerable Android device, you should patch it. But Google has only released fixes for the Android smartphones which it manufactures. If you own an Android made by another firm then you have to wait for them to push out a patch, and for it to be delivered by your carrier."

What Mr. Cluley shows before this quote is this table:

Issue	CVE	Severity
Remote Code Execution Vulnerability in Mediaserver	CVE-2015-6636	Critical
Elevation of Privilege Vulnerability in misc-sd driver	CVE-2015-6637	Critical
Elevation of Privilege Vulnerability in the Imagination Technologies driver	CVE-2015-6638	Critical
Elevation of Privilege Vulnerabilities in Trustzone	CVE-2015-6639	Critical
Elevation of Privilege Vulnerability in Kernel	CVE-2015-6640	Critical
Elevation of Privilege Vulnerability in Bluetooth	CVE-2015-6641	High
Information Disclosure Vulnerability in Kernel	CVE-2015-6642	High
Elevation of Privilege Vulnerability in Setup Wizard	CVE-2015-6643	Moderate
Elevation of Privilege Vulnerability in Wi-Fi	CVE-2015-5310	Moderate
Information Disclosure Vulnerability in Bouncy Castle	CVE-2015-6644	Moderate
Denial of Service Vulnerability in SyncManager	CVE-2015-6645	Moderate
Attack Surface Reduction for Nexus Kernels	CVE-2015-6646	Moderate

This lists the vulnerabilities, which are found in multiple versions of Android – from 4.4 KitKat to 6 Marshmallow. Now my Android tablet out-of-the-box is at 4.2 JellyBean. Before even trying to use my tablet I need to use the user community hacks to try and get updated to 4.4 KitKat, and a patched version of that release. I have no hope of going further than 4.4 KitKat with this device. (I only paid \$45 USD for it and just wanted to test it and verify that my decision to use iOS devices was

the way to go. Mission accomplished for me!)

Mr. Cluley concludes his article with this recommendation:

“When your device prompts you that a security update is available, be sure to apply it. If you aren’t one of the lucky ones to be told there is a security update, you should perhaps be having some strong words with your phone’s manufacturer – as maybe they need to be told that you’ll be less likely to buy one of their devices in future, if they can’t get a proper handle on keeping it updated.”

We could not agree more. If you received an Android device as a gift recently, or ‘treated’ yourself to one, do some research on your own. Get your device upgraded with the most recent patches you can. The security of your information on your device is your responsibility.

Caveat emptor. Buyer beware. I need to figure out what the Latin expression for ‘You get what you pay for’ is.

We believe we have found a real hot button for our readers and subscribers; securing private information. That’s one reason why we published a new report. [You’ll find many practical and useful tips in The Complete Guide to Computer Security... for Mere Mortals](#). The security and privacy of your personal information is within your control.

Planning and information gathering has already begun for a 2016 version of [The Complete Guide to Computer Security... for Mere Mortals](#). We plan to add a section on security for mobile devices; both Android and iOS devices. Watch for the announcement about the availability of the 2016 version of our security report.

Here is a video from Frederick D. our Computer Security Expert... See what he has to say here about Computer Security Solutions.

All thanks and credit for the above article must go to Graham Cluley for his article on [WeLiveSecurity.com](http://WeLiveSecurity.com).