

14 August 2007

By: Marius Oiaga, Technology News Editor



## [Mac OS X Leopard Is a Joke Compared to Windows Vista](#)

*Leopard hacked beyond recognition and not even out yet*

Apple applauds Mac OS X as the most secure and most advanced operating system in the world. Microsoft in turn has adopted a more modest marketing approach, in spite of the Wow campaign, and is comparing Windows Vista mainly with Windows XP. In terms of security Vista is just the safest Windows version available and nothing more. The same argument is not valid for Apple. With the Cupertino-based company it is all or nothing, which means that it's generally all. Just take the example of Safari 3 Beta browser for Windows. "Apple engineers designed Safari to be secure from day one," stated a message posted on the Apple official website. The reality? Security researchers turn up no less than 18 security vulnerabilities for Safari 3 in the browser's first day on 32-bit and 64-bit Windows Vista and Windows XP. Charles Miller from Independent Security Evaluators has really made a name for himself after he managed to hack the iPhone. Still, the security researcher from Independent Security Evaluators seems to have an affinity for fresh Apple products. Or at least this is the direction underscored by his presentation at Black Hat 2007 in [Las Vegas: "Hacking Leopard: Tools and Techniques for Attacking the Newest Mac OS X."](#) Miller cites Apple with the following: "Mac OS X delivers the highest level of security through the adoption of industry standards, open software development and wise architectural decisions." Security was also Apple's focus with Safari and iPhone and we have been able to see how well that turned up. But the upcoming release of Mac OS X, Leopard, scheduled for October 2007 is in a very poor condition in terms of security according to Miller. It is nothing but a joke compared to Windows Vista. And this is one aspect that emphasizes the differences between the next version of the world's most attacked platform and an operating system with an inexistent threat environment. Miller's conclusion is worrisome for future Leopard users: "Why Hacking Macs is Easy." According to Miller Macs are just as easy to hack as they are to use. "To help users, there are lots of 50+ suid root programs" revealed the security researcher. Suid Root is designed to help with the silent elevation of privileges in Unix and Unix based operating system such as the Mac OS X. Unix has had, a long time before Vista, access control capabilities, an equivalent to the User Account Control. Still, Suid Root is a design flaw, because allowing for silent and automatic elevation of privileges means inviting kernel level exploits. In contrast, nothing similar to the Unix setuid/suid or sudo functionality can be found in [the design of UAC in Vista](#). There is only one way that a service, application or process can gain elevation of privileges in Vista and that is only through the user. Moreover, Apple does not "bother users with burdensome updates." All the open source solutions included in Mac OS X are not kept up to date including OpenSSH, OpenSSL, Apache, Samba, Cups. "The Samba on Mac OS X had an exploitable remote root vulnerability in it...it hadn't been updated since February 2005," Miller stressed focusing on open source as an attack vector. But of course there's always the "safe from day one" Safari. Apple's browser, and by the way version 3 is going by default into Leopard, launches the following programs on execution: "Address Book, Finder, iChat, Script Editor, iTunes, Dictionary, Help Viewer, iCal, Keynote, Mail, iPhoto, QuickTime Player, Sherlock, Terminal, BOMArchiveHelper, Preview and DiskImageMounter." Any security vulnerability residing in any of these applications can be exploited via Safari. In the end Miller exposes Apple security for the joke that it is saying that the company "makes exploitation fun," mainly because creating exploits for Mac OS X is like going back in time to the software of 1999. The reason? "Apple doesn't randomize anything: the location of the stack, the location of the heap, the location of the binary image, the location of dynamic libraries and (to top it all off) heap is executable." By contrast Windows Vista introduces a security mitigation called

[Address Space Load Randomization \(ASLR\).](#)