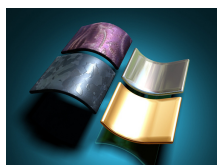


24 March 2007

By: Marius Oiaga, Technology News Editor

Windows logo  
Daniel F Pigatto

## [Windows vs. Linux vs. Mac OS X](#)

*Ignorance is bliss...*

There has been a consistent amount of "ink" spilled over comparing Windows, Linux and Mac OS X this month. The reports have generated some controversy, because they point out that Windows delivers a more secure platform than Linux and Mac OS X. For some, this simply appears to defy the "logic" that has been proliferated by marketing campaigns from Linux and Apple. Microsoft's own marketing campaigns always tout the latest Windows version as the most secure Windows platform to date, Linux and Apple just top that by offering an even more secure operating systems than Windows. There is the general customer perception that Linux and Mac OS X are not affected by bugs, or security vulnerabilities, that they are impervious and deliver absolute protection to their users. On more than one occasion, I have seen Linux and Mac OS X users claim that they never had to implement an anti-virus with their operating systems. This is the case of one of my friends, which never installed anything even remote to a security solution on her Mac OS X Tiger. So the fact that Linux and Mac OS X users feel safer than Windows users reflects a reality and not just a marketing doctrine. But at the same time you have to look at the statistics. On March 13, the Redmond Company released no security updates for any of its products. And while Microsoft was skipping a monthly patch cycle, the first time since 2005, on the very same day, Apple plugged a total of 45 security vulnerabilities in its operating system and in third party programs. The majority of security patches addressed issues reveled in January 2007 via the [Month of the Apple Bugs](#). In January, no less than 31 security vulnerabilities were disclosed for Apple products, at the rate of one per day. Has this scarred Apple's products in any way? I don't think so. Has it impacted Apple's reputation as a standard and an apex for security? Not even in the least. In fact, I have found that the majority of Mac OS X users remain unaware of this issue or even downplay it. And despite announcing their intention to contribute to the perfecting of Apple products, the two researchers behind the project, Kevin Finisterre of Digital Munition and L.M.H. from Month of Kernel Bugs, have been gratuitously attacked by Apple supporters. And we are down to the issue of patch development time. Symantec has looked into this issue and concluded that Microsoft Windows has a much shorter average patch development time than Red Hat Linux and Mac OS X. Symantec comprised statistics for 2006. Microsoft spent an average of 21 days on building updates for 39 security vulnerabilities in Windows, 12 of which were considered high severity in the last six months of the past year in comparison with the 13 days it took to deliver patches for 22 flaws in the first half of 2006, only five of which were labeled high severity. Red Hat Linux is runner up in the context of the shorter development time, taking almost three times as much as Microsoft to patch a sample set of 208 vulnerabilities from July to December 2006, only two of which were considered high severity. In the first six months of 2006, 42 vulnerabilities have been patched in Red Hat Linux, only one was considered high severity, and an average patch development time of 13 days was spent on delivering the fixes. 43 vulnerabilities plagued Mac OS X in the second half of 2006, one of which highly severe, and Apple took no less than an average patch development time of 66 days to resolve the issues. In the first six months of the past year, Apple had an average patch development time of 37 days for 21 vulnerabilities, three of which were considered high severity. In terms of the most critical vulnerabilities, Windows is clearly a more exposed platform with 17 high severity flaws in 2006. But since we are talking code quality, Windows had a total of 61 vulnerabilities in 2006, Red Hat Linux had 250, and Mac OS X 64. "The risk of exploitation in the wild is a major driving force in the development of patches. As with previous periods, Microsoft Windows was the operating

system that had the most vulnerabilities with associated exploit code and exploit activity in the wild. This may have pressured Microsoft to develop and issue patches more quickly than other vendors. Another pressure that may have influenced Microsoft's relatively short patch development time is the development of unofficial patches by third parties in response to high-profile vulnerabilities," Symantec explained in the [Symantec Internet Security Threat Report - Trends for July-December 06 -Volume XI, Published March 2007](#). Jeff Jones, Security Strategy Director in Microsoft's Trustworthy Computing group has compared the performances of [Windows Vista, Windows XP, Red Hat Linux and Mac OS X Tiger](#) in the first 90 days of commercial availability in terms of resolved vulnerabilities. Mac OS X v10.4 had 10 vulnerabilities disclosed prior to the April 29, 2005 launch, four of which high severity. In the first 90 days Apple patched 20 vulnerabilities in Mac OS X Tiger, eight of which, counting the four already mentioned were considered high severity. After the first 90 days there were still 17 issues expecting to be addressed in Mac OS X. Red Hat Enterprise Linux 4 Workstation shipped on February 15 2005, with 129 vulnerabilities publicly disclosed, no less than 40 high severity flaws. In the first 90 days of general availability Red Hat addressed a total of 181 vulnerabilities, 58 of which had a level of high severity. Microsoft resolved three vulnerabilities affecting Internet Explorer before it shipped Windows XP SP2. Including these three, Microsoft plugged a total of 14 holes, out of which eight were high severity. Windows Vista delivered a superior performance to Windows XP SP2 with only five vulnerability disclosures in the first 90 days since November 30, 2006. "5 total vulnerability disclosures in the first 90 days, with one of them fixed and one High severity one pending, along with 2 Mediums and a Low severity vulnerability. Is that good, bad or indifferent? Let's look at other operating systems and see if they can provide some context for these numbers," Jones revealed.Q.E.D.