

31 March 2008

By: Marius Oiaga, Technology News Editor



Mac OS X 10.5
Leopard
Apple

[Microsoft Finds Irony in Mac OS X Getting Hacked Before Vista SP1](#)

Courtesy of Jeff Jones, Strategy Director in the Microsoft Security Technology Unit

Microsoft was not without a reaction to the past week's events at [CanSecWest Vancouver 2008](#). The conference's PWN2OWN 2008 hacking challenge sponsored by TippingPoint involved three machines and just as many operating systems, VAIO VGN-TZ37CN running Ubuntu 7.10, Fujitsu U810 running Vista Ultimate SP1 and MacBook Air running OSX 10.5.2. In the first day of the contest, when hackers were permitted only network attacks all the platforms held their own. But starting with day two, Mac OS X Leopard fell within two minutes. On day three, Vista SP1 was hacked after a few hours, while Ubuntu managed to get through intact. Jeff Jones, Strategy Director in the Microsoft Security Technology Unit, commented on the fact that Leopard, a product that is heavily advertised as being more secure than Windows Vista, was the first to fall. Apparently, flawless marketing campaigns do not equal secure offerings. Apple has learned this the hard way. "Okay, having said that, given how obnoxious and misleading I find those Mac OS X ads and how they've spent millions of dollars publicly criticizing Windows Vista security improvements, I find it ironic and apropos that Mac OS X was the first machine to be owned in the PWN 2 OWN contest at CanSecWest. Charlie Miller appears to have set up a web site containing malicious code and used a 'browse to own' vulnerability to win the contest," [Jones stated](#). Charlie Miller, with Independent Security Evaluators (ISE), is the hacker that claimed a \$10,000 prize and a MacBook Air, and revealed to [ComputerWorld](#) that he and his team chose to own Leopard because it was less of a challenge than Vista SP1 or Ubuntu. Miller exploited a zero-day vulnerability in Safari 3.1. "It was the easiest one of the three. We wanted to spend as little time as possible coming up with an exploit, so we picked Mac OS X. We sat down about three weeks ago and decided we wanted to throw our hats into the ring. It took us a couple of days to find something, then the rest of the week to work up an exploit and test it. It took us maybe a week altogether," Miller stated. On the third day of CanSecWest 2008, [Vista SP1 Ultimate was also hacked](#), but not through a hole in the operating system's components. A zero-day vulnerability in Adobe's Flash was exploited in order to compromise Vista.