

[Vista Ultimate SP1 and Ubuntu Shame the Ultra-Hackable Mac OS X 10.5 Leopard](#)

Apple's OS hacked in just 2 minutes

Windows Vista Ultimate Service Pack 1 and Ubuntu 7.10 have bested the Apple proprietary platform in terms of security, by shaming the ultra-hackable Mac OS X 10.5 Leopard. There is a constant face-off on the operating system market, not only when it comes down to the install base and audience, but also security-wise. While the general perspective is that Windows operating systems deliver no contest to the security offered by Linux and Mac OS X platforms, the reality might be a tad different than the claims provided by bulletproof marketing campaigns or fanatic culture. Case in point: the CanSecWest PWN2OWN 2008 hacking contest claimed its first victim, the fully patched Mac OS X 10.5.2 running on the "thinnovative" MacBook Air.

Apple's official description of MacBook Air reads "ultrathin, ultraportable, and ultra unlike anything else." Obviously, the Cupertino-based security company also meant ultra-hackable. And the description of Mac OS X 10.5 Leopard is nothing more than an example of arrogance defying a sad reality, Apple is placing its own customers at risk by advertising Leopard as a panacea for security issues. "Security. Safer by design. Every Mac is secure — right out of the box — thanks to the proven foundation of Mac OS X." It took a team of three security researchers under 2 minutes to hack a fully patched copy of Mac OS X 10.5.2 Leopard running on a MacBook Air machine.

"At 12:38pm local time, the team of Charlie Miller, Jake Honoroff, and Mark Daniel from Independent Security Evaluators have successfully compromised the Apple MacBook Air, winning the laptop and \$10,000 from TippingPoint's Zero Day Initiative. They were able to exploit a brand new 0day vulnerability in Apple's Safari web browser. Coincidentally, Apple has just started to ship Safari to some Windows machines, with its iTunes update service. The vulnerability has been acquired by the Zero Day Initiative, and has been responsibly disclosed to Apple who is now working on the issue. Until Apple releases a patch for this issue, neither we nor the contestants will be giving out any additional information about the vulnerability. You can track the vulnerability on the Zero Day Initiative upcoming advisories page under ZDI-CAN-303," reads [the official announcement](#) from Tipping Point.

In the CanSecWest PWN2OWN 2008 contest, hackers had a go at three machines: 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 challenge sponsored by TippingPoint's Zero Day Initiative, no computer could be breached, as the organizers only allowed attacks over a network. The second day of the hacking contest allowed attackers to direct CanSecWest organizers to visit webpages or open messages in Leopard's email client. Charlie Miller, the security expert who hacked the iPhone in 2007, owned the MacBook Air box via a zero-day vulnerability that was disclosed only to Apple. It took Miller just 2 minutes to hack OS X Leopard.

"So Dragos [Dragos Rui, the conference's organizer] just announced before lunch that within 10 minutes of opening Day 2 of the pwn2own contest - the Mac has fallen. Wonder what took so long? Just talked with Dragos - the finder is signing with ZDI to get paid - so no vuln details for us. But we DO know that there was no 3rd party software on the box yet so the 0-day is in some inbox software," stated [Robert Hensing](#), Microsoft Security Software Engineer.