

19 March 2009

By: Marius Oiaga, Technology News Editor

Charlie Miller
Terri Forslof

[IE8, Firefox, Safari Owned via 0-Day Vulns, Chrome Survives Intact](#)

At the CanSecWest Vancouver 2009 Pwn2Own contest

[Internet Explorer 8](#), Firefox and Safari were all owned via zero-day vulnerabilities in the first day of the CanSecWest Vancouver 2009 Pwn2Own contest. The competition organizers offered to contestants two machines, a Sony Vaio running Microsoft's Windows 7, and pre-installed with IE8, Firefox and Chrome, the other a Mac with Safari and Firefox. Both computers featured the default software installations and no additional plugins were made available. Scenarios on which the end user visits a link pointing them to malicious content were allowed. Safari fell first, and it fell hard.

"Charlie Miller got the luck of the draw, and had the first time slot for the browser competition. His target- Safari on Mac OS X. Before I could even pull my camera out, it was over within 2 minutes- and Charlie (coincidentally also last year's first winner of the day) is now the proud owner of yet another MacBook, and \$5,000 from the Zero Day Initiative," revealed [Terri Forslof](#), Manager of Security Response for TippingPoint.

Actually, reports from people present at the event indicate that the Mac was hacked via a previously undisclosed vulnerability affecting the Safari browser in just 10 seconds. This is a new record for Miller, who hacked the Mac in two minutes at the 2008 Pwn2Own. But Miller was outstaged by another contestant, known only as Nils.

"With a little tweaking, he ran a sleek exploit against IE8, defying Microsoft's latest built in protection technologies- DEP (Data Execution Prevention) as well as ASLR (Address Space Layout Randomization) to take home the Sony Vaio and \$5,000 from ZDI," Forslof added. "If that wasn't enough, Nils pulled a Safari exploit out of his hat (perhaps the same one used for the drawing?) and wowed us a second time- quickly taking down Apple's browser for another cool \$5,000."

But Nils failed to stop here. He also owned [Firefox](#) by exploiting another 0-day vulnerability, winning a total of \$15,000. At the end of the first day of the Pwn2Own contest, [Google Chrome](#) was the last browser standing, left completely intact.

Internet Explorer 8 (IE8) RTW is available for download [here](#) (for 32-bit and 64-bit flavors of Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008).

The latest release of Google Chrome is available for download [here](#).

Firefox 3.1 Beta 3 for Windows is available [here](#).

Firefox 3.1 Beta 3 for Linux is available [here](#).

Firefox 3.1 Beta 3 for Mac OS X is available [here](#).