

12 June 2007

By: Marius Oiaga, Technology News Editor



[Safari on Windows - First Day - First Vulnerabilities! Already under Attack!](#)

Welcome to the most attacked platform in the world

It's raining zero-day vulnerabilities for the [Apple Safari browser](#) as an official welcome to the most attacked platform in the world. On June 11 2007, Apple Chief Executive Officer Steve Jobs took Safari - the native browser for the Mac platform - out of its safe heaven and cast it onto the wild Windows operating systems, Windows Vista and XP to be more specific. But just hours following the availability of Safari for Vista and XP, independent security researchers have set up to rain on Safari's Windows parade with a collection of vulnerabilities. Apple has touted Safari for Windows in the same manner as Mac OS X, applauding the high default security level of the browser. "Security. Now you can enjoy worry-free web browsing on any computer. Apple engineers designed Safari to be secure from day one," reads a message posted on the Safari webpage. Well, three independent security researchers took the challenge and on Safari's first day on Windows, they managed to come up with a total of eight vulnerabilities affecting Apple's browser. "On the download page Apple write: "Apple engineers designed Safari to be secure from day one". So, I've decided to take it for a test drive, and ran Hamachi. I wasn't surprised to get a nice crash few minutes later... A first glance at the debugger showed me that this memory corruption might be exploitable, although I'll have to dig more to be sure of that. Again, this is just a beta version. But don't you hate those pathetic claims?" asked [Aviv Raff On .NET](#). But he is not alone in this endeavor. [David Maynor](#) a security expert with Errata Security uncovered six vulnerabilities in Safari in a single afternoon. Maynor informed that four flaws permit Denial of Service attacks while the remaining two are critical vulnerabilities as they allow for remote code execution. Both David Maynor and Aviv Raff have highlighted their vulnerabilities through fuzz testing. By contrast, [Thor Larholm](#), also a security researcher, took a more traditional approach when he identified a zero-day vulnerability in Safari in just two hours. "I downloaded and installed Safari for Windows 2 hours ago, and I now have a fully functional command execution vulnerability, triggered without user interaction simply by visiting a web site. The logic behind this vulnerability is quite simple and the vulnerability class has been known and understood for years, namely that of protocol handler command injection. URL protocol handlers on the Windows platform work by executing a process with specific command line arguments. When Apple released Safari for the Windows platform they neglected to implement a proper level of input validation for these arguments, which means that you can break out of the intended confines and wreak havoc," Larholm revealed.