

3 July 2008

By: Marius Oiaga, Technology News Editor

[Microsoft Parades Internet Explorer 8 Beta 2 Features](#)

Beta 2 is planned to drop this August

Internet Explorer 8
Microsoft

Microsoft is stepping up its game when it comes down to [Internet Explorer 8](#), signaling that the release of the next development milestone of the browser is getting closer and closer. IE8 Beta 2 will be made available next month, in August 2008, with the build advertised as a consumer-oriented release. While [Beta 1 dropped in March 2008](#) was focused on web content developers and designers, Beta 2 will deliver goodies for end users, or at least this is the promise from Microsoft. In this context, one thing that the IE team had been hard at work was hammering away at IE8 in order to bulletproof the browser as much as possible. Starting with Beta 2, Internet Explorer 8 will deliver a plethora of security features and improvements designed to mark the evolution from IE7 in terms of user protection. The Redmond giant has effectively classified threats into three categories, namely Web Application Vulnerabilities, Browser & Add-on Vulnerabilities, and Social Engineering Threats and, consequently, added extra mitigations to IE8. "As we were planning Internet Explorer 8, our security teams looked closely at the common attacks in the wild and the trends that suggest where attackers will be focusing their attention next. While we were building new Security features, we also worked hard to ensure that powerful new features (like Activities and Web Slices) minimize attack surface and don't provide attackers with new targets," explained [Eric Lawrence](#), Program Manager Internet Explorer Security. The additional security layers will provide tiered in-depth protection to IE8 users beyond what IE7 is capable of offering today. According to Lawrence, IE8 will enable Safer Mashups, including the sanitization process of HTML and JavaScript Object Notation. Internet Explorer 8 has been tweaked to sniff all downloads for their MIME type and determine the actual content of the files grabbed by end users from servers across the web. On top of the extra security tiers designed to address risks from web-based applications, Microsoft is also delivering enhancements to features such as Protected Mode, ActiveX Opt-in, and Zone Lockdowns, already available in IE7. In this regard, IE8 will feature DEP/NX Memory Protection, an improved Protect Mode API, Application Protocol Prompt, File Upload Control and even Social Engineering Defenses. And with the XSS-based attacks on the rise, IE8 Beta 2 will introduce the XSS Filter. "XSS vulnerabilities enable an attacker to control the relationship between a user and a web site or web application that they trust. Cross-site scripting can enable attacks such as: cookie theft, including the theft of session cookies that can lead to account hijacking; monitoring keystrokes input to the victim web site / application; and performing actions on the victim web site on behalf of the victim user. For example, an XSS attack on Windows Live Mail might enable an attacker to read and forward e-mail messages, set new calendar appointments, etc." explained [David Ross](#), IE Security Software Engineer. And last but definitely not least, IE8 Beta 2 comes with the SmartScreen Filter, complete with malware protection. The SmartScreen Filter is the evolution of the Phishing Filter, but at the same time, it is so much more, offering an overhauled user interface, boosted performance, enhanced heuristics & telemetry, and even support for Anti-Malware, according to Lawrence. "The SmartScreen Filter goes beyond anti-phishing to help block sites that are known to distribute malware, malicious software that attempts to attack your computer or steal your personal information. The SmartScreen anti-malware feature is URL-reputation-based, which means that it evaluates the servers hosting downloads to determine if those servers are known to distribute unsafe content. SmartScreen's reputation-based analysis works in concert with other signature-based anti-malware technologies like the Malicious Software Removal Tool, Windows Defender, and Windows Live OneCare, in order to provide comprehensive

protection against malicious software," Lawrence [added](#).