

By: Philip 2008, Apple News Editor

[Safari 3.1.1 Fixes PWN 2 OWN Flaw and Other Security Issues](#)

Mozilla Firefox also patched

Updates are now available for Safari and Firefox (Mac and Windows) users. Both [Safari 3.1.1](#) and FireFox [2.0.0.14](#) address security issues. As some of you may have already hinted, with the release of Safari 3.1.1, Apple has patched [the flaw](#) Charlie Miller used to win 10 Gs and a MacBook Air in the PWN 2 OWN contest at CanSecWest. Other security issues concerning Tiger (10.4.11) and Leopard (10.5.2) have been covered with Safari 3.1.1, as well as two security issues affecting Windows XP/Vista users. **MACCVE-2008-1026** Apple notes that it has fixed the issue where a maliciously crafted web page may lead to an unexpected application termination or arbitrary code execution, mentioning a heap buffer overflow in WebKit's handling of JavaScript regular expressions as the cause. The issue may be triggered via JavaScript when processing regular expressions with large, nested repetition counts. This may lead to an unexpected application termination or arbitrary code execution, Apple says. Safari 3.1.1 addresses the issue by performing additional validation of JavaScript regular expressions. Apple credits Charlie Miller for reporting the issues. **CVE-2008-1025** The patch fixes an issue where a malicious website may result in cross-site scripting: "An issue exists in WebKit's handling of URLs containing a colon character in the host name. Opening a maliciously crafted URL may lead to a cross-site scripting attack. This update addresses the issue through improved handling of URLs," Apple notes. **WINDOWSCVE-2007-2398** and **CVE-2008-1024** As far as Windows users running Safari are concerned, the patches address issues where a maliciously crafted website that can control the contents of the address bar (patched in a public beta of v3.0 and reintroduced with v3.1) and an issue where a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution due to a memory corruption issue exists in Safari's file downloading respectively. "By enticing a user to download a file with a maliciously crafted name, an attacker may cause an unexpected application termination or arbitrary code execution. This update addresses the issue through improved handling of file downloads. This issue does not affect Mac OS X systems," Apple says. Apple recommends that all Safari users update to the latest version of the company's standard web browser. Click [HERE](#) to download.