

19 February 2007

By: Marius Oiaga, Technology News Editor

IE7 and Firefox 2.0 Share Vulnerabilities

Exploits require user interaction



Internet Explorer 7 and Firefox 2.0 share a logic flaw. The issue is actually more severe, as the two versions of the Microsoft and Mozilla browsers are not the only ones affected. In this regard, the vulnerability impacts Internet Explorer 5.01, Internet Explorer 6 and Internet Explorer 7 but also Firefox 1.5.0.9. Microsoft has stressed the fact that IE7 on Windows Vista is not affected in any manner. "In all modern browsers, form fields (used to upload user-specified files to a remote server) enjoy some added protection meant to prevent scripts from arbitrarily choosing local files to be sent, and automatically submitting the form without user knowledge. For example, ".value" parameter cannot be set or changed, and any changes to .type reset the contents of the field," said Michal Zalewski, the person that discovered the IE7 flaw. User interaction is a must if both vulnerabilities are to be successfully exploited. In this context, the user would have to enter text in malformed areas on a web page, either from IE or Firefox. Zalewski explained that the keyboard input in unrelated locations can be selectively geared toward input fields by the attacker. In order to access the demonstration of the IE7 vulnerability click [here](#). A similar demonstration for Firefox can be found [here](#). "Both examples are Windows-specific, and require C:BOOT.INI to exist and be readable by users. The attack itself is not limited to a particular operating system, but I decided to provide a demonstration for the most popular desktop OS - *nix versions that access /etc/hosts or /etc/passwd are easy to develop," Zalewski added.