By: Marius Oiaga, Technology News Editor

The First Internet Explorer 7 Vulnerability

Truth or hoax?

The report of a vulnerability affecting Internet Explorer 7, in fact the first vulnerability in IE7, has been around for quite some time, but I have just came across it. In fact, the vulnerability was initially reported on November 1, 2006. As far I was unable to confirm its authenticity from my usual sources, and this is explanatory for the subtitle. But I am also going to go on a limb and call it a hoax. I will explain why, just bear with me. According the flaw report, Internet Explorer 7 is vulnerable to DLL-load hijacking. "When IE7 is executed it will load several DLL files. While trying to load some of those files, it does not provide the full path of the DLL file to the function which loads the DLL file to the memory, and therefore Windows will search for this file in the user's machine using the directories provided in the PATH environment variable, and will load the first match it will found," reported Aviv Raff.In this context, for the browser to actually load a malicious DLL or the downloader DLL of a malicious file, the file in question must first of be planted via a process that bypasses the generic detection of startup folder and startup registry keys alterations by security software, in one of the PATH directories. On the next launch of Internet Explorer 7, the browser will load and execute the malicious DLL. Let me translate this. This scenario involves an already compromised system. In fact Microsoft's response to this is: "If the attacker can put a dll on the box in a location that is in the user's PATH variable, then they already own the box." Otherwise Internet Explorer 7 is not impacted by the DLL-load hijacking vulnerability. Time is another factor. This report is over a month old and the fact that exploits are hesitating to appear is proof that IE7 DLL-load hijacking is a hoax. Additionally, Windows would not limit the search to the directories provided in the PATH environment, but to an array of locations that differ in concordance with the enabled/disabled status of SafeDllSearchMode. These are the locations searched: the directory from which the application loaded, the system directory, the 16-bit system directory, the current directory and the directories that are listed in the PATH environment variable.

Copyright (c) 2001-2008 Softpedia. All rights reserved. Softpedia™ and Softpedia™ logo are registered trademarks of SoftNews NET SRL.