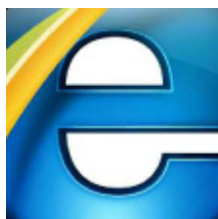


16 May 2008

By: Marius Oiaga, Technology News Editor

Internet Explorer
Microsoft

[IE8 Beta 1 Attack Code Available in the Wild](#)

Internet Explorer "Print Table of Links" cross-zone scripting vulnerability

Security researcher [Aviv Raff](#) has released an example of attack code for Internet Explorer 7 and Internet Explorer 8 Beta 1 in the wild. According to Raff Microsoft's Internet Explorer browser is vulnerable to exploits targeting a Cross-Zone Scripting security flaw that affects the "Print Table of Links" feature. Under normal conditions, via "Print Table of Links", users are able to print not only a webpage but also a table with all the links on the page in an appendix. "An attacker can easily add a specially crafted link to a webpage (e.g. at his own website, comments in blogs, social networks, Wikipedia, etc.), so whenever a user will print this webpage with this feature enabled, the attacker will be able to run arbitrary code on the user's machine (i.e. in order to take control over the machine)", Raff explained. According to the Israeli security researcher the vulnerability can be exploited on IE7 and IE8 Beta 1 running on Windows XP, in such a manner that an attacker could gain complete control over the operating system. The User Account Control mitigation built into Windows Vista prevents complete take-over of the platform, allowing only for information leakage. Raff managed not only to detail the vulnerability but also to make the proof-of-concept available for download. Microsoft was informed of the flaw last week but so far failed to deliver a patch. "Whenever a user prints a page, Internet Explorer uses a local resource script which generates a new HTML to be printed. This HTML consists of the following elements: Header, webpage body, Footer, and if enabled, also the table of links in the webpage. While the script takes only the text within the link's inner data, it does not validate the URL of links, and add it to the HTML as it is. This allows to inject a script that will be executed when the new HTML will be generated", Raff added.