

Re: Vista's Security Rendered Completely Useless by New Exploit

Source:

<http://www.tech-archive.net/Archive/Vista/microsoft.public.windows.vista.general/2008-08/msg03764.html>

- *From:* johngalt <guest@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 11 Aug 2008 19:32:57 -0500
-

The proof, but Warp 10 is not gonna like it:

["http://arstechnica.com/news.ars/post/20080811-the-sky-isnt-falling-a-look-at-a-new-vista-security-bypass.html"](http://arstechnica.com/news.ars/post/20080811-the-sky-isnt-falling-a-look-at-a-new-vista-security-bypass.html)

Wrote:

The sky isn't falling: a look at a new Vista security bypass

(<http://arstechnica.com/news.ars/post/20080811-the-sky-isnt-falling-a-look-at-a-new-vista-security-byp>

By 'Peter Bright' (<http://arstechnica.com/authors.ars/PeterB>) |

Published: August 11, 2008 - 07:30AM CT

One of the papers presented at the 'Black Hat USA 2008'

(<http://www.blackhat.com/>) security conference was an analysis a number of the protection mechanisms built into Windows Vista and Windows Server 2008 that are designed to make it harder to convert software bugs into security flaws. '-How to Impress Girls with Browser Memory Protection Bypasses-' (<http://taossa.com/archive/bh08sotirovdowd.pdf>), authored by security researchers Mark Dowd at IBM and Alexander Sotirov at VMware, presented a number of attacks against Vista's various security features in isolation, and then attacks that could disable multiple protections all together. Put together, the result is that Vista's mitigation mechanisms are circumvented, making buggy software exploitable.

The security features being bypassed are all intended to minimize the impact of 'buffer overflows'

(http://en.wikipedia.org/wiki/Buffer_overflow). Buffer overflows are a particular kind of programming error that occur when a program attempts to store too much data in the buffer allocated for the data. This causes anything following the buffer to be overwritten. Buffer overflows are exploitable when it's possible to insert arbitrary executable code into a process and then make that code run. If an attacker can do this then the attacker has gained the ability to do whatever he likes to the