

27 November 2008

By: Marius Oiaga, Technology News Editor

[Office 2007 Service Pack 2 More Secure than SP1](#)

Vista not the only product with 50% less vulnerabilities

Office
Microsoft

In order to support applauding the security enhancements in Windows Vista, Microsoft has played the vulnerability counting game on more than one occasion, comparing the volume of security flaws in the latest edition of the Windows client with previous releases, and even with Linux and Mac OS X.

However, Windows Vista is not the sole example of the Redmond company managing to slash the number of vulnerabilities in half. The same is the case with the software giant's other flagship product, Office 2007. [David LeBlanc](#), a senior software development engineer at Microsoft, offered internal statistics from Microsoft on a range of Office editions, taking into consideration CVE entries and bulletin count from 9/18/2007 to 11/17/2008.

"While we did a lot of good work to try and make Office 2003 more secure than previous versions, against the attacks we're seeing in 2007, it wasn't any better than Office XP," LeBlanc stated.

"Now, if you factor in huge amounts of work (no magic, no silver bullet, just lots and lots of work) that we did fixing fuzz bugs in Office 2007 and Office 2003 SP3, it looks like we've cut the incoming vulnerability rate by approximately half. If we look at it app-by-app, I think PowerPoint is a clear winner - they've had 5 CVE entries for older versions and only 1 for PowerPoint 2007 since 1/1/2007! Word has also done very well, dropping from 11 and 12 CVE entries, in prior versions, to only 2 for Word 2007, over the same period."

The CVE count for [Office 2007 SP1](#) was of just 16 items in approximately one year, while that for the RTM version of the system was of 19. In fact, Office 2003 SP3 and Office 2007 RTM were almost on a par in this regard. However, for releases preceding Office 2003 SP3, the CVE count was almost double. LeBlanc stated that Microsoft was committed to continuing to improve security for the Office System with the next release, namely SP2 for Office 2007.

"It will be interesting to see how much additional gain that gives us. I'd like to see us do even better over time - while we've clearly made some significant gains, we still have more work remaining. We are currently doing about as many fuzzing iterations per weekend as we're required to do to meet SDL requirements for the entire product cycle (to be fair, the requirement is for clean runs, and we're not there yet, and when we do get there, we use a different fuzzer). We've done twice as many fuzz iterations against Office 2007 SP2 as we did against Office 2007 during the entire product cycle, and 4x more against Office 14 than against Office 2007," LeBlanc stated.

Office 2007 SP1 is available for download [here](#).

Office 2003 SP3 is available for download [here](#).