

20 February 2008

By: Marius Oiaga, Technology News Editor

[64-bit Vista Natively Bulletproofed Against Heap-Based Buffer Overruns](#)

Unlike the 32-bit editions



When it comes down to the 32-bit Windows Vista vs. 64-bit Windows Vista, the comparison generally focuses on the added benefits synonymous with handling system memory. Because the address space of 64-bit Vista is not limited to 4GB, users are able to use a maximum of 128 GB of RAM with the Ultimate, Business and Enterprise SKUS. But at the same time, there are added benefits, and one of them is in terms of security. The 64-bit editions of Vista come to the table with PatchGuard (Kernel Patch Protection), Address Space Layout Randomization (ASLR), Heap and Stack randomization, and even heap corruption detection. As far as Heap Based Buffer Overruns are concerned, both 32-bit and 64-bit Vista offer protection, but only in the x64 versions of the operating system is the even heap corruption detection enabled by default. Michael Howard, Senior Security Program Manager in the Security Engineering group at Microsoft, explained that, in x86 Vista, software developers have to call the HeapSetInformation API in order to enable heap corruption detection. "The HeapSetInformation function (...) lets your application configure the Windows heap manager with a small number of options. The only security-related setting kills your application in case of heap corruption. A 'heap corruption' is anything that messes with data in the Windows heap, for example damaged caused by a buffer overrun, writing to a stray pointer or a double-free are examples. Assume you code has a heap-based buffer overrun that you do not know about (because if you knew about it, you'd remove it!) If an attacker attempts to exploit it, there is a reasonable chance the attack might make the application crash rather than running exploit code," Howard explained. In the eventuality that Vista will detect a heap corruption, the operating system will simply fail the application. In 32-bit Vista this will only happen if the developer has called the HeapSetInformation API. In contrast, Vista x64 not only will detect heap-based buffer overruns by default, but will also offer protection against additional illegal operations involving heaps. "There is no need to call this API, the operating system enables termination-on-corruption by default. But you should call it anyway, because your code might run on 32-bit Windows. By default, all 64-bit applications running on 64-bit Windows Vista or Windows Server 2008 get this defense by default, there is no need to call the function. A 32-bit application running on 64-bit Windows does not get the defense for free, the code must call the function," Howard added.