

11 April 2008

By: Marius Oiaga, Technology News Editor

[XP SP3 Safe from Vista RTM and SP1 Fountain of Vulnerabilities](#)

And from the flaws



Windows XP -
Windows Vista
Microsoft

With the advent of Windows Vista RTM, the public perception focused on XP SP2's superiority and further development of the two platforms comes to support such a scenario, despite Microsoft's claims of the contrary. The Vista RTM vs. XP SP2 face-off has now translated to the comparison between Windows XP Service Pack 3 and Windows Vista SP1. And despite the fact that Vista was applauded as an apex of security (because of the Security Development Lifecycle), with SP1 designed to carry the evolution onward, it is Windows XP SP3 who manages to prove itself on the front lines of attacks. The third and final service pack for XP is safe from the fountain of vulnerabilities that has affected Windows Vista Gold and SP1. In fact, the Microsoft Windows graphics device interface failed to get even a single drop on XP SP3. On April 8, 2008, Microsoft patched a [couple of privately reported vulnerabilities in GDI](#). The flaws, according to the Redmond company, have been labeled with a maximum severity rating of Critical because they allow for remote code execution and the complete takeover of a compromised system in the eventuality of a successful exploit. However, even though all Windows operating systems are vulnerable to attacks via malformed EMF, or WMF image files, including Vista RTM and Vista SP1, XP SP3 is safe. "All currently supported Windows systems are at risk. Windows XP Service Pack 3 is not affected by this vulnerability," Microsoft [informed](#). "A client-side remote code execution vulnerability affects GDI due to how it handles integer calculations [and file name parameters]. An attacker can exploit this issue by tricking an unsuspecting victim into opening a malicious EMF or WMF file. A successful attack will result in the execution of arbitrary attacker-supplied code in the context of the currently logged-in user. It may also be possible to exploit this issue in the context of SYSTEM; this will result in a complete compromise," explained Rob Keith, Symantec Security Response Engineer. But this is not the first time that the GDI has been a source of vulnerabilities for the Windows platform, or for Windows Vista. The fact of the matter is that approximately one year ago, Microsoft was releasing an [out-of-band set of patches](#) for no less than seven security vulnerabilities in the Windows graphics device interface. Back in April 2007, two of the vulnerabilities in GDI were also connected with the Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats. However, it was the Windows Animated Cursor remote code execution Critical vulnerability that caused quite a stir, because of the impact it had on Windows Vista RTM. At that time, [McAfee demonstrated a Vista suicide](#) via a malicious animated cursor (.ani file) targeting the zero-day GDI flaw in the operating system. Cupertino-based security company Symantec has detected attacks tailored to the new EMF or WMF vulnerabilities in the GDI. Symantec Researcher Sean Hittel stated that: "It has been less than two days since Microsoft announced a couple of vulnerabilities in graphics device interface (GDI) EMF formatted images, but our DeepSight honeypots are already showing some signs of exploitation in the wild. Although the exploits that we have seen so far do not yet appear to be functional, they appear to have the right general idea in their exploitation. It is possible that these exploits either have been leaked and are 'in-work' copies, or that they are functional on some platform that we have not tested. However, the exploit (named 'top.jpg') does contain functional payload, which downloads a secondary file (word.gif)."