

3 March 2007

By: Marius Oiaga, Technology News Editor



Tamper Detection

## **BIOS Validation Failures on Windows Vista Machines**

### *Windows Vista Tamper Detection*

Users may be prompted to activate Windows Vista on machines on which activating the operating system was not previously required. This is a paraphrase of a Knowledge Base article from Microsoft addressing an issue from late January that was updated the past month. According to Microsoft, the issue may be encountered when users install a device driver and when they install, run or remove a program. "This problem can occur because a specific system setting is deleted when a program runs with administrative credentials. The removal of this setting may cause a BIOS validation check to fail; the BIOS validation check is part of the system activation process for PCs from major manufacturers. This behavior causes a regular genuine validation check that occurs at boot time to fail. Therefore, the customer may be prompted to activate Windows Vista, even though the system did not previously require activation," said Alex Kochis, senior product manager of WGA (Windows Genuine Advantage). Microsoft revealed that handling products from household names will generate issues, and Kochis gave the examples of nProtect GameGuard, Trend Micro Internet Security, PC-Cillin Anti-Virus and PC Tools Spyware Doctor. In order to resolve the problem, access Microsoft's KB article 931573. "This issue highlights the importance of the new tamper detection technology enabled by the Software Protection Platform in Windows Vista. When evidence of system tampering is detected the system will go into a non-genuine or tampered state depending on the tamper. Also, depending on the severity of tampering the remedies for it can range from a simple reboot all the way to a complete re-install. In this particular case, the programs in question delete a specific system setting that triggers the tamper detection," Kochis added. Microsoft underlined the importance of tampering checks as an integer part of the operating system, due to the fact that, while they might cause minor inconvenience to users, they ensure the integrity of Windows Vista. The only shortcoming of the integrity checks is the fact that they cannot distinguish between accidental and intentional tamperings.