

10 April 2007

By: Marius Oiaga, Technology News Editor

[Microsoft Confirms Windows Vista OEM BIOS Crack](#)

And says that it will tackle the issue



Microsoft confirmed the fact that hackers have developed a valid Windows Vista crack designed to exploit the operating system's OEM BIOS activation. Alex Kochis, a senior licensing manager with the WGA team revealed that the OEM Activation was a measure introduced concomitantly with Windows XP and designed to streamline the deployment and activation process of the operating system. "Microsoft worked with OEMs to develop an implementation that would work best for them and their customers while keeping the goals of product activation clearly in focus. As we looked to develop a solution, it was important to ensure that product activation technology could still deliver an acceptable degree of protection, while at the same time, reduce the need for an extra step by the end user," Kochis revealed. The Redmond Company introduced a marker in the BIOS of the OEM's motherboard that identifies OEM systems. Via this action, Microsoft managed to intimately connect Windows with a value in the BIOS of the motherboard, and with an OEM machine and an OEM licensed operating system. "Over the years we've seen examples of BIOS editors that, with some work, allowed people to make an edited BIOS appear to be an OEM BIOS. Because Windows Vista can't be pirated as easily as Windows XP, it's possible that the increased pressure will result in more interest in efforts to hack the OEM Activation 2.0 implementation," Kochis opined. As of now, Microsoft revealed that it is aware of two cracks that exploit the Windows Vista OEM 2.0 activation. One method is essentially the same as the OEM cracks implemented in Windows XP and it involves editing the BIOS of a motherboard in order to masquerade the motherboard as an OEM product. Kochis classified the process as labor-intensive and risky due to the fact that users can render the motherboard completely useless. "So while this method works today, it's potentially hazardous and really doesn't scale well to large numbers of systems, which makes it less of a threat," Kochis added. As far as the second OEM workaround is concerned, Kochis promised that Microsoft will have little trouble in tackling it as it simply involves a software crack designed to make Windows Vista believe that it is running on OEM hardware. "We focus on hacks that pose threats to our customers, partners and products. It's worth noting we also prioritize our responses, because not every attempt deserves the same level of response. Our goal isn't to stop every "mad scientist" that's on a mission to hack Windows. Our first goal is to disrupt the business model of organized counterfeiters and protect users from becoming unknowing victims. This means focusing on responding to hacks that are scalable and can easily be commercialized, thereby making victims out of well-intentioned customers," Kochis concluded.