

30 March 2007

By: Marius Oiaga, Technology News Editor



[Windows Vista Suicide, Courtesy of McAfee](#)

Animated cursors kill Vista

Windows Vista, Microsoft's extensively applauded most secure Windows platform to date can be taken down by nothing more than a mere animated cursor. I have seen this piece of news spreading, following a security advisory posted by the Microsoft Security Response Center. But what is the real deal behind this information? Microsoft has warned that it is aware of limited and targeted attacks impacting a critical vulnerability in Microsoft Windows Animated cursor handling. At the basis of the zero-day vulnerability is insufficient format validation, before cursors, animated cursors, and icon rendering. Security company Symantec informed that in the eventuality of a successful exploit, the attacker will be able to perform remote arbitrary code execution on the victim's machine. There are two vectors for this kind of attack, one is the Internet browser and the other is the desktop email client. "In order for this attack to be carried out, a user must either visit a Web site that contains a Web page that is used to exploit the vulnerability or view a specially crafted e-mail message or email attachment sent to them by an attacker," according to Microsoft Security Advisory (935423). The zero-day Windows Animated Cursor Handling vulnerability affects a set of Windows editions including Windows Vista. Because it allows for remote code execution, the .ani files vulnerability will automatically receive the highest severity rating from Microsoft, namely Critical. The Redmond Company will not downgrade the severity level of this vulnerability for Windows Vista, although the operating system has a few mitigations in place that do not expose users as much as other editions of Windows. "Customers who are using Internet Explorer 7 on Windows Vista are protected from currently known web based attacks due to Internet Explorer 7.0 protected mode. If you are reading Outlook 2007 you are protected regardless of if you are reading the mail as plain text or not. If you are reading email using Windows Mail on Vista you are protected as long as you are not forwarding or replying to the attacker's email," Microsoft informed. However, despite these mitigations, Windows Vista is very much vulnerable to attacks. In the video embedded at the bottom, you will be able to see Craig Schmugar, virus research manager with McAfee, send Windows Vista into a perpetual "crash-restart" loop by simply dragging a malformed .ani file to the operating system's desktop.