

The update will be released worldwide simultaneously in 23 languages for all affected versions of Windows once it passes a series of rigorous testing procedures. It will be available on Microsoft's Download Center, as well as through Microsoft Update and Windows Update. Customers who use Windows' Automatic Updates feature will be delivered the fix automatically.

Based on strong customer feedback, all Microsoft's security updates must pass a series of quality tests, including testing by third parties, to assure customers that they can be deployed effectively in all languages and for all versions of the Windows platform with minimum down time.

Microsoft has been carefully monitoring the attempted exploitation of the WMF vulnerability since it became public last week, through its own forensic capabilities and through partnerships within the industry and law enforcement. Although the issue is serious and malicious attacks are being attempted, Microsoft's intelligence sources indicate that the attacks are limited in scope and are not widespread.

In addition, anti-virus companies indicate that attacks based on exploiting the WMF vulnerability are being effectively mitigated through up-to-date signatures.

Customers are encouraged to keep their anti-virus software up-to-date. The Microsoft Windows AntiSpyware (Beta) can also help protect your system from spyware and other potentially unwanted software. Customers can also visit Windows Live Safety Center and are encouraged to use the Complete Scan option to check for and remove malicious software that takes advantage of this vulnerability. We will continue to investigate these public reports.

If you are a Windows OneCare user and your current status is green, you are already protected from known malware that uses this vulnerability to attempt to attack systems.

Customers who follow safe browsing best practices are not likely to be compromised by any exploitation of the WMF vulnerability. Users should take care not to visit unfamiliar or un-trusted Web sites that could potentially host the malicious code.

Microsoft encourages users to exercise caution when they open e-mail and links in e-mail from untrusted sources. While we have not encountered any situation in which simply opening an email can result in attack, clicking on a link in an email could result in navigation to a malicious site. For more information about Safe Browsing, visit the Trustworthy Computing Web site.

The intentional use of exploit code, in any form, to cause damage to computer users is a criminal offense. Accordingly, Microsoft continues to assist law enforcement with its investigation of the attacks in this case.

Customers who believe they have been attacked should contact their local FBI office or post their complaint on the Internet Fraud Complaint Center Web site. Customers outside the U.S. should contact the national law enforcement

agency in their country.

We continue to encourage customers to follow our Protect Your PC guidance of enabling a firewall, applying software updates and installing antivirus software. Customers can learn more about these steps at the Protect Your PC Web site.

Customers who believe they may have been affected by this issue can also contact Product Support Services. You can contact Product Support Services in the United States and Canada at no charge using the PC Safety line (1 866-PCSAFETY). Customers outside of the United States and Canada can locate the number for no-charge virus support by visiting the Microsoft Help and Support Web site.

Mitigating Factors:

. In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail or Instant Messenger request that takes users to the attacker's Web site.

. In an e-mail based attack involving the current exploit, customers would have to click on a link in a malicious e-mail or open an attachment that exploits the vulnerability. It is important to remember that this malicious attachment may not be a .wmf. It could also be a .jpg, .gif, or other format. At this point, no attachment has been identified in which a user can be attacked simply by reading mail.

. An attacker who successfully exploited this vulnerability could only gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

. By default, Internet Explorer on Windows Server 2003, on Windows Server 2003 Service Pack 1, on Windows Server 2003 with Service Pack 1 for Itanium-based Systems, and on Windows Server 2003 x64 Edition runs in a restricted mode that is known as Enhanced Security Configuration. This mode mitigates this vulnerability where the e-mail vector is concerned although clicking on a link would still put users at risk. In Windows Server 2003, Microsoft Outlook Express uses plain text for reading and sending messages by default. When replying to an e-mail message that is sent in another format, the response is formatted in plain text. See the FAQ section of this vulnerability for more information about Internet Explorer Enhanced Security Configuration.

—
Russ Grover
Small Business IT Support
SBS Rocks!
Portland/Beaverton OR
Email: Sales at [SmallBusinessITSupport.com](mailto:Sales@SmallBusinessITSupport.com)
Website: <http://www.SmallBusinessITSupport.com>

-
- Prev by Date: ***Re: QuickBooks Pro 2006 on SBS 2003 Nightmare***
 - Next by Date: ***Re: Understanding sbs backup errors***
 - Previous by thread: ***Internet Authentication Service Issues***
 - Next by thread: ***Re: Remote Desktop vs VPN***
 - Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***