



VULNERABILITY AFFECTS ALL VERSIONS OF WINDOWS OPERATING SYSTEMS

Jan. 9, 2006

Source: Kathy Bergsma
(352) 392-2061
kbergsma@ufl.edu

GAINESVILLE, Fla. --- University of Florida information technology experts want users of Windows operating systems to be aware of a serious vulnerability that was discovered in Windows Meta File (WMF) during the holidays. It impacts all versions of all Windows operating systems and is being exploited across the world affecting many Windows file types and applications.

By simply visiting Web sites, opening e-mails or reading instant messages to view infected images, users can expose themselves to viruses, worms and spyware. It is more important than ever to use discretion and ensure trust when opening e-mail, surfing the web, messaging or using other network applications, experts warn.

"This vulnerability is particularly hazardous," said Kathy Bergsma, UF information security manager. "There are many different vectors by which it can be exploited making it difficult for antivirus products to detect."

The University of Florida IT Security Team offers a Web site where UF students, faculty and staff can test computers for the vulnerability. For more information and a link to the test, visit <http://infosec.ufl.edu/wmf/>.

Microsoft issued a patch on Jan. 5. Users running Microsoft Windows should visit <http://windowsupdate.microsoft.com> to apply this computer fix immediately. While at this site, users can also verify that their Windows Automatic Updates control (right side of page) is on, thus confirming that all future patches released will be updated to their computer.

Bergsma said there are several viruses spread through e-mail, instant messaging and malicious Web sites that exploit the WMF vulnerability. "User vigilance is critical to prevent compromise; only they can safeguard their computer," she added.

Microsoft's advisory can be found at:
<http://www.microsoft.com/technet/security/advisory/912840.mspx>.