Microsoft issued information on 12 new security bulletins

Today, Microsoft issued information on 12 new security bulletins. The following summary provides Symantec's evaluation of two of the most critical issues.Vulnerability in Microsoft Malware Protection Engine.Symantec Security Response rates the Microsoft Malware Engine vulnerability to be the most critical of the security bulletins. This remote code execution vulnerability has affected various Microsoft products that include the Malware Protection Engine, including Windows Live OneCare, Microsoft Antigen 9.x, Microsoft Windows Defender, Microsoft ForeFront Security for Microsoft Exchange Server 1.x, and Microsoft ForeFront Security for SharePoint Server 1.x. This vulnerability occurs when Microsoft's AntiVirus client that uses the Microsoft Malware Protection Engine is configured to allow PDF file processing. This vulnerability is critical since the malicious PDF could be hosted on a Web site or distributed via e-mail where it could be scanned by the infected AV engine at the gateway or when it arrives at the desktop. A successful exploit will completely compromise the affected computer.Vulnerabilities in Microsoft WordMicrosoft also issued patches for multiple vulnerabilities in Microsoft Word, which corrects the zero-day Word vulnerabilities associated with Trojan.Mdropper.T/W/X, which are Trojan horses that attempt to drop additional threats on the compromised computer. This bulletin also includes a patch for a client-side code execution vulnerability in Microsoft Word that can be triggered by a malformed object embedded within a document. A successful exploit could let a remote attacker execute arbitrary code in the context of the currently logged in user."Symantec continues to track the increasing trend of zero-day vulnerabilities and this months critical vulnerabilities noted in Microsoft Word point to that trend," said Vince Hwang, group product manager, Symantec Security Response. "As hackers continue to close the gap between disclosing and exploiting vulnerabilities, Symantec recommends that both enterprises and consumers actively update their software with patches as soon as they are available."Symantec recommends the following actions for IT administrators:· Evaluate the possible impact of these vulnerabilities to critical systems.· Plan for required responses including patch deployment and implementation of security best practices using the appropriate security and availability solutions.· Take proactive steps to protect the integrity of networks and information.· Verify that appropriate data backup processes and safeguards are in place and effective.· Remind users to exercise caution in opening all unknown or unexpected e-mail attachments and in following Web links from unknown or unverified sources.Symantec recommends the following actions for consumers:· Regularly run Windows Update and install the latest security patches to keep software up to date.· Avoid opening unknown or unexpected e-mail attachments or following Web links from unknown or unverified sources.* Use an Internet security solution such as Norton Internet Security 2007 to protect against today's known threats and tomorrow's Internet security risks.Additional information will be available on Symantec's Security Response Blog shortly at:http://www.symantec.com/enterprise/security_response/weblog/ <http://www.symantec.com/enterprise/security_response/weblog/> Additional information on Microsoft's security bulletins can be found at:http://www.microsoft.com/technet/security/bulletin/ms07-feb.mspx <http://www.microsoft.com/technet/security/bulletin/ms07-feb.mspx> Symantec's security experts will closely monitor further information related to these vulnerabilities and will provide updates and security content as necessary. Please let me know if you have any questions or if you are interested in speaking with a Symantec expert on any of the above vulnerabilities.