Today, Microsoft issued information on six security bulletins. The following summary provides Symantec Security Response

Vulnerability in Workstation Service Memory CorruptionSymantec Security Response rates the vulnerability in Microsoft's Workstation Service Memory to be the most critical of the security bulletins this month. A successful exploitation of this vulnerability could result in a complete system compromise. This issue can be exploited by remote anonymous attackers on Windows 2000, Windows XP and possibly Windows Server 2003 systems. A wide variety of component technologies and services are impacted by this issue which has potential for a worm-style attack.Vulnerability in Microsoft XML Core Services Symantec Security Response rates the Microsoft XML Core Services vulnerability to be critical as well. The Microsoft XML Core Services technology allows developers to create XML-enabled applications. All supported versions of Internet Explorer (including the new Internet Explorer 7.0) make use of this functionality and are susceptible to possible attack. This is a publicly known vulnerability that is currently being exploited in the wild. "Many of the issues addressed in this month's batch of patches attend to publicly exploited issues," said Alfred Huger, senior director of development, Symantec Security Response. "Attackers are exploiting vulnerabilities with increasing speed, and it's imperative that computer users protect themselves by installing updated software patches as quickly as possible."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 Microsoft Update and install the latest security updates 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 to protect against today's known and tomorrow's unknown threats.Additional information will be available on Symantec's Security Response Blog shortly at: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/ms06-nov.mspxSymantec'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.