

Dear Microsoft Partner,

We are contacting you today to make you aware that we have released Microsoft Security Bulletin MS03-039 today, September 10, 2003. This bulletin details three critical vulnerabilities in the Windows operating system and provides instructions for applying the corresponding patch. While there is currently no active exploit of this vulnerability, if successfully exploited, these vulnerabilities would allow an attacker to gain control of the target system.

After ensuring your own systems are secure, we strongly encourage you to help your customers obtain and deploy this patch to any affected system that connects to their infrastructure, including systems on a local area network and remote or mobile systems. For the most current information on affected systems and recommended remediation steps, please read the bulletin posted at: <http://go.microsoft.com/?linkid=248305>

We understand the potential effect this situation and the recommended remediation steps may have on your customers. Microsoft is committed to providing them with information and tools to help run their enterprise safely and reliably on an on-going basis. When we become aware of vulnerabilities, it is our goal to quickly share protection and remediation information and work in partnership with you to eliminate these kinds of threats to their business. In order to help protect their computing environment from security vulnerabilities, we strongly encourage you to recommend they visit <http://go.microsoft.com/?linkid=248306> and implement the following three steps in their enterprise:

1. Verify firewall configuration.

Audit Internet and intranet firewalls to ensure they comply with your customers' security policy; these are their first line of defense. In addition, evaluate using host-level firewalls such as the Internet Connection Firewall in Windows XP. This is especially important for systems such as laptops and home PCs that connect to your customers' network remotely.

2. Stay up to date.

Use update services from Microsoft to keep their systems up-to-date. These services include three main components:

* Automatic Updates, available on Windows XP, Windows 2000 SP3 and SP4, and Windows Server 2003. Automatic Updates works with the Windows Update Web site to automate the process of updating Windows systems.

* Software Update Services (SUS), a patch-distribution server available for download from our Web site. SUS enables you deploy a server in your enterprise that Automatic Updates clients will use to get only approved and tested patches.

* Systems Management Server (SMS) is a flexible, enterprise-wide software update and systems management product.

In addition to using these update services, we strongly recommend that your customers subscribe to Microsoft's free security notification service at <http://go.microsoft.com/?linkid=248307>, so that they are proactively kept aware of new security issues.

3. Use and keep antivirus software up-to-date.

Antivirus software programs will help protect their systems against many viruses, worms, Trojan horses, and other malicious code. To protect systems from new viruses, it's also important to obtain up-to-date antivirus signatures through a subscription service from the antivirus software vendor. Your customers should not let remote users or laptops connect to their network unless they have up-to-date antivirus software installed. In addition, recommend your customers use antivirus software in multiple points of their computer infrastructure, such as on edge Web proxy systems, as well as on email servers and gateways.

You can also protect your customers' networks by recommending they require employees to take the same three steps above with home and laptop PCs they use to remotely connect to their enterprise, and by encouraging them to talk with friends and family to do the same with their PCs. To make this easier, we have set up a new Web site to assist PC users at <http://go.microsoft.com/?linkid=248308>.

Again, we want to encourage you to read this security bulletin and help your customers deploy the patch to their systems. We want to thank you for your patience and work with you to protect your business and your customers' businesses from these kinds of security threats.

Thank you,

Microsoft Corporation