

[NT] Security Enhancements in Windows XP Service Pack 2

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0016.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 06/06/04

To: list@securiteam.com

Date: 6 Jun 2004 20:00:57 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Security Enhancements in Windows XP Service Pack 2

SUMMARY

Microsoft plans to publish a second service pack for Microsoft Windows XP which was released in 2001. "Windows XP Service Pack 2 addresses new challenges to the security of personal computers by making a number of basic improvements to the operating system".

DETAILS

The following review of Windows XP Service Pack 2 security enhancements is based on the white paper released by Microsoft and other information from Microsoft's web site. The article is divided to two parts, the first reviews the technical changes applied in the Service Pack, and the second reviews the implications on users, system administrators' databases and developers.

Network Security:

Network protection is the largest area of improvement in Windows XP Service Pack 2, and the one with the most implications for existing software.

Securiteam: [NT] Security Enhancements in Windows XP Service Pack 2

Improved Windows Firewall (Previously known as Internet Connection Firewall, or ICF), has been changed to a stateful filtering firewall, and is enabled by default. The new firewall turns on very early in the system boot cycle, before the network stack is fully enabled, reducing the possibility of intrusions during the boot cycle. It also turns off very late in the shutdown cycle, after the network stack has been disabled, reducing the possibility of intrusions during system shutdown. Windows Firewall is now enabled for all network interfaces by default, has a convenient control panel graphical user interface to enable exceptions by application, and can be placed under administrative control in a domain through new Group Policy settings. In addition, the netsh command-line tool, which was added to Windows XP in the Advanced Networking Pack to support IPv6, has been enhanced to support Windows Firewall configuration.

The Remote Procedure Call (RPC) service has been made less vulnerable to outside attack, and new permission levels have been added to allow administrators to control which RPC servers are blocked, which are exposed only to the local subnet, and which are exposed to the entire network. Windows Firewall has been enhanced to support these permissions, and to limit port openings from alleged RPC servers based on the security context in which they run.

The Distributed Component Object Model (DCOM) infrastructure has additional access control restrictions to reduce the risk of a successful network attack. By default, only authenticated administrators can remotely activate and launch COM components, and only authenticated users can remotely call COM components. Administrators can apply fine control to individual services to allow only appropriate users to use the services, or to restrict services to local use.

Local Security:

NX memory pages:

On CPUs that support execution protection (NX) technology, Windows XP Service Pack 2 marks data pages non-executable. This feature of the underlying hardware prevents execution of code from pages marked in this way. This prevents attackers from overrunning a marked data buffer with code and then executing the code; it would have stopped the Blaster worm dead in its tracks. The only processor families that currently support NX are the 64-bit AMD K8 and Intel Itanium; however, Microsoft expects future 32-bit and 64-bit processors to provide hardware based execution protection.

Sandboxing:

In addition to supporting NX, Service Pack 2 implements sandboxing. All binaries in the system have been recompiled with buffer security checks enabled to allow the runtime libraries to catch most stack buffer overruns, and "cookies" have been added to the heap to allow the runtime libraries to catch most heap buffer overruns.

Application Security:

Outlook Express: In SP2, a new version of Outlook Express can block images and other external content in HTML email, warn about other applications

Securiteam: [NT] Security Enhancements in Windows XP Service Pack 2

trying to send mail, and control the saving and opening of attachments that could potentially be a virus. Outlook Express also coordinates with the new application execution service, to better protect the system from the execution of harmful attachments. Users also have the option to read or preview all messages in plain text mode, which can avoid potentially unsafe HTML. Windows Messenger and MSN Messenger share the improvements to attachment control made for Outlook Express.

Internet Explorer (IE) has been made much more secure in Service Pack 2.

It now manages add-ons and detects crashes due to add-ons, controls whether or not binary behaviors are allowed to run, and applies the same safety restrictions to all URL objects that previously applied only to ActiveX controls. It has more control over the execution of all content. It dramatically restricts the capabilities of the Local Machine zone, to block attacks that attempt to use local content to run malicious HTML code. IE now requires that all file-type information provided by Web servers be consistent, and "sniffs" files for malicious code trying to masquerade as a benign file type.

IE now disallows access to cached scriptable objects: HTML pages can only script their own objects. This better blocks attacks on the IE cross-domain security model, disallowing scripts that listen to events or content in other frames, such as a script that might try to capture credit card information from a form. IE now has a built-in facility to block unwanted pop-up windows, and manage the viewing of desired pop-up windows. It can block all signed content from an untrusted publisher, will block signed code with invalid digital signatures by default, and will only display one prompt per control per page. Further, IE now keeps scripts from moving or resizing windows and status bars to hide them from view or obscure other windows.

The Alerter and Messenger services, which are sometimes used by administrators and developers to communicate over a network, have been disabled by default in Windows XP Service Pack 2.

DirectX 9 and Windows Media Player 9 both contain security, performance, and functionality improvements. For more information about improvements to DirectX, consult the DirectX home page at <http://www.microsoft.com/windows/directx/>. For more information about improvements to Windows Media Player, refer to the Windows Media Player home page at <http://www.microsoft.com/windows/windowsmedia/>.

Patch Management:

Windows Update Version 5. An Express Install option makes it easy for users to quickly get just the critical and security updates they need, and an Automatic Updates control panel makes updating a set-and-forget task instead of a constant chore. In addition, Microsoft has endeavored to make most new patches smaller than they have been in the past, although Service Pack 2 is itself huge.

Security Center provides a central location for information about the

Securiteam: [NT] Security Enhancements in Windows XP Service Pack 2

security of your computer, with an easy-to-use graphical interface. Windows Installer 3.0 provides more security options for software installation, and provides patch management infrastructure that helps to keep patches small through "delta compression" technology. Windows Installer 3.0 helps to avoid the downloading of unneeded, superseded or obsolete patches, and supports patch removal reliably.

Implications of the Improvements in the Service Pack 2:

User Immigration:

For users, the most common adjustments have to do with allowing exceptions to the improved security (i.e. each application which requires network connection needs to be unblocked). A popup security alert dialog whenever they run a new application that wants to act as an Internet server. Users will need to think about whether they want to grant each application this privilege, but they only have to think about it once, and they can change their minds easily later.

Antivirus Reminder:

Users will also find that Security Center nags them a bit if they lack an AntiVirus program, if their AntiVirus signatures are out of date, if they ignore critical system updates, or if they turn off their firewall. Most users will find this extra vigilance by the operating system more of a comfort than an annoyance; knowledgeable users can turn off any incorrect warnings by telling Security Center about their third-party security applications.

Administrator Adjust:

Administrators will need to explicitly allow access to server applications on their networks. Since access can be limited to the local subnet or allowed from any source, administrators have more control than ever before. Administrators and other IT professionals should read about this in detail on the Windows XP SP2 Web site, paying specific attention to <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwxp/html/securityinxpsp2.asp> <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwxp/html/securityinxpsp2.asp>.

Effect on Developers:

Windows and Web application developers will have to revisit distributed applications that use RPCs or DCOM. They may also have to apply patches to their development tools and allow their tools Windows Firewall privileges to allow remote debugging to work.

How does Windows XP SP2 affect SQL Server?

SQL Server will have access to the local subnet by means of file and print sharing, which will enable access to named pipes, also known as multi-protocol, that use Port 445. TCP/IP and UDP will be turned off by default. Applications that connect to a SQL Server database by means of a network will not be able to accept or make connections. This setting change helps protect the customer system by making it resilient to malicious worms that send port requests to a computer in an attempt to create a denial of service attack.

Securiteam: [NT] Security Enhancements in Windows XP Service Pack 2

ADDITIONAL INFORMATION

The white paper can be found at:

<<http://download.microsoft.com/download/6/6/c/66c20c86-dcbe-4dde-bbf2-ab1fe9130a97/windows%20xp%20sp%20white%20paper.doc>>

The SQL FAQ document can be found at:

<<http://www.microsoft.com/sql/techinfo/administration/2000/security/winxpsp2faq.asp>>
<<http://www.microsoft.com/sql/techinfo/administration/2000/security/winxpsp2faq.asp>>

Visit the

<<http://www.microsoft.com/technet/prodtechnol/winxppro/sp2preview.mspx>>

Windows XP Service Pack 2 homepage for more information.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.