


Securing A Clean Installation Of Windows XP/Vista/7

 **Original** | **No Header, No Background, No Images**

For: [Windows XP](#) | [Windows Vista](#) | [Windows 7](#)

Last Updated: 10May12 | Published: 14Jan04 | Status: To Be Continued

1. Introduction

- 1.1. [Windows Vulnerabilities](#)
- 1.2. [Security Updates For Windows](#)
- 1.3. [Windows Service Packs](#)
- 1.4. [Securing A Clean Installation Of Windows](#)

2. On The Security Updates For Windows Released After The Latest Windows Service Pack

- 2.1. [Listing The Microsoft Security Bulletins Released After The Latest Windows Service Pack](#)
- 2.2. [Identifying The Security Updates For Windows That Resolve Windows Vulnerabilities That Require User Interaction To Be Exploited](#)
- 2.3. [Identifying The Security Updates For Windows That Resolve Windows Vulnerabilities That Do Not Require User Interaction To Be Exploited](#)

3. Preparing For Securing A Clean Installation Of Windows XP/Vista/7

- 3.1. [Preparing For Securing A Clean Installation Of Windows XP](#)
- 3.2. [Preparing For Securing A Clean Installation Of Windows Vista](#)
- 3.3. [Preparing For Securing A Clean Installation Of Windows 7](#)

4. Securing A Clean Installation Of Windows XP/Vista/7

- 4.1. [Securing A Clean Installation Of Windows XP](#)
- 4.2. [Securing A Clean Installation Of Windows Vista](#)
- 4.3. [Securing A Clean Installation Of Windows 7](#)

5. Additional Reading

1. Introduction

i

- Windows XP was initially released as a 32-bit (a.k.a., x86) operating system. Three years later a 64-bit (a.k.a., x64) version of Windows XP, Windows XP Professional x64, was released. Windows XP Professional x64, however, was derived from Windows Server 2003, not the initial Windows XP, and, therefore, shares Windows vulnerabilities, Windows Service Packs, and Security Updates for Windows with Windows Server 2003 x64, not Windows XP x86. For additional information, see [Additional Reading \(below\)](#).
- In this page, securing a clean installation of Windows XP/Vista/7 includes Windows XP (all editions) x86, Windows Vista (all editions) x86 and x64, and Windows 7 (all editions) x86 and x64, not Windows XP Professional x64.
- If you install a 32-bit version of Windows Vista/7, then install 32-bit Windows Service Packs and 32-bit Security Updates for Windows. If you install a 64-bit version of Windows Vista/7, then install 64-bit Windows Service Packs and 64-bit Security Updates for Windows.
- A clean installation of Windows is an installation of Windows to a partition that does not have Windows installed on it. A clean installation of Windows includes an installation of Windows to a new hard disk, to a newly created partition, or to a partition wiped of its existing installation of Windows. A clean installation of Windows is in contrast to an upgrade installation of Windows. An upgrade installation of Windows is an installation of Windows to a partition that overwrites an existing installation of Windows with either a more advanced edition of Windows or a newer version of Windows.
- Only a clean installation of Windows, not an upgrade installation of Windows, is guaranteed to be free from compromise, and, therefore, can be secured.
- In this page, Windows Service Packs and Security Updates for Windows must be copied to removable media for offline installation. Since files copied to CDs/DVDs are less susceptible to viruses than files copied to external hard disk drives and flash memory drives, CDs/DVDs are the removable media of choice in this page.

1.1. Windows Vulnerabilities

Windows vulnerabilities are flaws in the Windows operating system code that render Windows susceptible to exploitation. The successful exploitation of a Windows vulnerability results in compromise. Toward securing Windows, it is instructive to divide Windows vulnerabilities into two groups: 1.) those that require user interaction to be exploited, and 2.) those that do not require user interaction to be exploited.

For the Windows vulnerabilities that require user interaction to be exploited, compromise requires user interaction with the computer besides placing the computer online. User interactions with the computer that can result in compromise, known as triggers, include visiting Web sites, receiving/opening emails, opening email attachments, creating/accessing shares, opening/running/installing shared files, accessing/opening/running/installing downloaded or otherwise acquired files, etc.. In other words, for the Windows vulnerabilities that require user interaction to be exploited, in the absence of the appropriate user interaction required to trigger exploitation, compromise cannot occur upon placing the computer online.

For the Windows vulnerabilities that do not require user interaction to be exploited, compromise does not require any user interaction with the computer besides placing the computer online. In other words, for the Windows vulnerabilities that do not require user interaction to be exploited, there is no trigger and compromise can occur upon placing the computer online.

i

- Placing a computer online means connecting it to a network (i.e., an Intranet and/or the Internet, wired and/or wireless).
- This page assumes:
 - a router is not used when connecting to the Internet and/or worms that can bridge routers, such as Downadup (a.k.a., Conficker), are in the wild.
 - Intranets include a compromised computer and/or a malicious user that is attempting to compromise the other computers connected to the Intranet.
 - your ISP and/or network administrator is not filtering, or is doing a poor job of filtering, malicious network traffic.

After installing Windows, a typical user places the computer online and runs Windows Update or Microsoft Update (Windows/Microsoft Update). Although the intention - to update and secure Windows - is well founded, the practice is unfortunate because worms exist that compromise Windows without the need for user interaction.

Worms are the class of threat that attempt to copy themselves from computer to computer over a network. Worms have been created that successfully exploit the Windows vulnerabilities that do not require user interaction to be exploited. In other words, worms exist that compromise Windows without the need for user interaction. Worms that compromise Windows without the need for user interaction are extremely dangerous because they can automatically spread across and comprise networked Windows computers as soon as they are placed online. Worms that compromise Windows without the need for user interaction are mentioned on the evening news and include the infamous [W32.Blaster.Worm \(symantec.com\)](#), [W32.Welchia.Worm \(a.k.a., Nachi\) \(symantec.com\)](#), [W32.Sasser.Worm \(symantec.com\)](#), and [W32.Downadup \(a.k.a., Conficker\) \(symantec.com\)](#). Moreover, Blaster, Welchia, Sasser, and Downadup remain so prevalent that even today - years after the worms were discovered - Windows computers are still being compromised by these worms as soon as they are placed online, including during the time that Windows/Microsoft Update is running.

i

Vulnerabilities are sometimes classified according to whether or not they are "wormable." A vulnerability is wormable if it does not require user interaction to be exploited. In other words, a vulnerability is wormable if it can be exploited upon placing the computer online. A vulnerability is not wormable if it requires user interaction to be exploited. In other words, a vulnerability is not wormable if, in the absence of the appropriate user interaction required to trigger exploitation, it cannot be exploited upon placing the computer online.

1.2. Security Updates for Windows

Microsoft releases a Microsoft Security Bulletin Summary on the second Tuesday of each month (a.k.a., Patch Tuesday). A Microsoft Security Bulletin Summary consists of one or more Microsoft Security Bulletins. A Microsoft Security Bulletin describes one or more newly discovered vulnerabilities in a Microsoft product and links to a Security Update file (a.k.a., patch) which resolves the vulnerabilities upon being installed.

i

Microsoft Security Bulletins are assigned an alpha-numeric name with syntax, MS##-###, where MS## is the year, and -### is the Microsoft Security Bulletin released that year. For example, MS10-001 is the first Microsoft Security Bulletin released in 2010.

Security Updates for Windows are dependent upon the version of Windows and the Windows Service Pack level. Therefore, the installation of a Security Update for Windows resolves a newly discovered Windows vulnerability, or group of related Windows vulnerabilities, in a particular version of Windows at a particular Windows Service Pack level.

Security Updates for Windows can be installed through Windows/Microsoft Update. In this page, however, some Security Updates for Windows must be downloaded and copied to removable media for offline installation, which is only possible through the Microsoft Download Center as linked to in the Microsoft Security Bulletins.

1.3. Windows Service Packs

Microsoft typically releases a Windows Service Pack (SP) for the newer versions of Windows every 12-24 months. A Windows Service Pack is a single file that contains multiple previously released Updates for Windows, Security Updates for Windows, and sometimes new features for a particular version of Windows. Therefore, the installation of a Windows Service Pack resolves multiple previously discovered Windows vulnerabilities in a particular version of Windows.

Eventually, multiple Windows Service Packs are released for a version of Windows. Some Windows Service Packs are fully cumulative and, therefore, do not require the installation of a previous Windows Service Pack. Some Windows Service Packs are not cumulative, or are only partially cumulative, and, therefore, require the installation of a previous Windows Service Pack.

Windows XP/Vista/7 Service Packs And Previous Service Pack Requirements	
Windows Service Pack	Requires Installation Of Previous Windows Service Pack
XP SP1	-
XP SP2	None
XP SP3	XP SP1 or XP SP2
Vista SP1	-
Vista SP2	Vista SP1
7 SP1	-

Windows Service Packs have a cutoff date for the inclusion of Updates for Windows, Security Updates for Windows, new features, etc. into the Windows Service Pack. Security Updates for Windows released before the cutoff date are included in the Windows Service Pack. Security Updates for Windows released after the cutoff date are not included in the Windows Service Pack.

After the cutoff date is set, the Windows Service Pack is built and tested. Windows Service Pack testing can take a month or longer, after which the Windows Service Pack is released. Since Security Updates for Windows are likely to be released during Windows Service Pack testing, it is worth noting that the Windows Service Pack cutoff date, not the Windows Service Pack release date, determines which Security Updates for Windows are included in a Windows Service Pack.

Latest Windows XP/Vista/7 Service Packs, Release Dates, Cutoff Dates, And Includes Through Security Update				
Windows	Latest Service Pack	Release Date	Cutoff Date	Includes Through Security Update
XP	SP3	06May08	~08Apr08	MS08-025
Vista	SP2	26May09	~14Apr09	MS09-015
7	SP1	22Feb11	~31Dec10	MS10-101

Windows Service Packs can be installed through Windows/Microsoft Update. In this page, however, Windows Service Packs must be downloaded and copied to removable media for offline installation, which is only possible through the Microsoft Download Center.

1.4. Securing A Clean Installation Of Windows

In this page, securing Windows means to resolve the known Windows vulnerabilities before they can be exploited. Toward securing Windows, it is instructive to divide Windows vulnerabilities into two groups: 1.) those that require user interaction to be exploited, and 2.) those that do not require user interaction to be exploited.

The Windows vulnerabilities that do not require user interaction to be exploited, since worms exist that successfully exploit them, must be resolved offline (i.e., before placing the computer online). The Windows vulnerabilities that require user interaction to be exploited, provided the user has not interacted with the computer in a way that could result in compromise, (e.g., by visiting Web sites, receiving/opening emails, opening email attachments, creating/accessing shares, opening/running/installing shared files, accessing/opening/running/installing downloaded or otherwise acquired files, etc.), can be resolved by placing the computer online and running Windows/Microsoft Update.

The following steps resolve the known Windows vulnerabilities before they can be exploited, thereby, securing a clean installation of Windows:

1. Perform the following offline, and before interacting with the computer in a way that could result in compromise:
 1. A clean installation of Windows
 2. Install the Windows Service Packs that bring your installation of Windows to the latest Windows Service Pack level. (This resolves the old Windows vulnerabilities that are wormable and not wormable.)
 3. Install the Security Updates for Windows released after the latest Windows Service Pack that resolve Windows vulnerabilities that do not require user interaction to be exploited. (This resolves the newly discovered Windows vulnerabilities that are wormable.)
2. Perform the following online, and before interacting with the computer in a way that could result in compromise:
 1. Run Windows/Microsoft Update and install the Security Updates for Windows. (This resolves the newly discovered Windows vulnerabilities that are not wormable.)

2. On The Security Updates For Windows Released After The Latest Windows Service Pack



- The Windows vulnerability severity rating (low, moderate, important, and critical) and security impact (denial of service, elevation of privilege, information disclosure, remote code execution, and spoofing) are not important. The only important thing is whether the Windows vulnerability requires, or does not require user interaction to be exploited.

- A Microsoft Security Bulletin may address multiple Windows vulnerabilities. If any of the Windows vulnerabilities addressed in Microsoft Security Bulletin do not require user interaction to be exploited, then the Security Update for Windows must be installed offline.

2.1. Listing The Microsoft Security Bulletins Released After The Latest Windows Service Pack

One of the steps in securing a clean installation of Windows is to install the Security Updates for Windows released after the latest Windows Service Pack that resolve Windows vulnerabilities that do not require user interaction to be exploited. To do this, it is necessary to know which Microsoft Security Bulletins were released after the latest Windows Service Pack. The following lists the Microsoft Security Bulletins released after the latest Windows Service Pack:

1. Visit the [Search Microsoft Security Bulletins \(technet.microsoft.com\)](http://technet.microsoft.com) page.
2. In the Product/Technology dropdown, select the version of Windows that you intend to install.
3. In the Service Pack dropdown, select the latest Window Service Pack.
4. Check **Show only bulletins that contain updates that have not been replaced by a more recent update..**
5. For Update Severity Rating, check **Critical**, check **Important**, check **Moderate**, and check **Low**.
6. In the Bulletin release date dropdown, select **All**.
7. Click **Go**.
8. The Microsoft Security Bulletins released after the latest Windows Service Pack are listed for the version of Windows that you intend to install.

2.2. Identifying The Security Updates For Windows That Resolve Windows Vulnerabilities That Require User Interaction To Be Exploited

One of the steps in securing a clean installation of Windows is to install the Security Updates for Windows released after the latest Windows Service Pack that resolve Windows vulnerabilities that do not require user interaction to be exploited. To do this, it is necessary to identify the Security Updates for Windows that resolve Windows vulnerabilities that require, or do not require user interaction to be exploited. The following language examples from Microsoft Security Bulletins identify Security Updates for Windows that resolve Windows vulnerabilities that require user interaction to be exploited:

- *"This vulnerability requires that a user be logged on and visiting a Web site for any malicious action to occur."* - Microsoft Security Bulletin MS10-035.
- *"An attacker could exploit the vulnerability by constructing a specially crafted Web page."* - Microsoft Security Bulletin MS10-053.
- *"This vulnerability requires that a user open a specially crafted media file or receive specially crafted streaming content from a Web site or any application that delivers Web content."* - Microsoft Security Bulletin MS10-062.
- *"An attacker could host a malicious Web site that hosts specially crafted media content that is designed to exploit this vulnerability through an internet browser and then convince a user to view the Web site and open the specially crafted media content."* - Microsoft Security Bulletin MS10-062.
- *"In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site."* - Microsoft Security Bulletin MS10-053.
- *"An attacker could host a specially crafted Web site that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the Web site. The attacker could also take advantage of compromised Web sites and Web sites that accept or host user-provided content or advertisements. These Web sites could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by clicking a link in an e-mail message or in an Instant Messenger message that takes users to the attacker's Web site, or by opening an attachment sent through e-mail."* - Microsoft Security Bulletin MS10-053.
- *"In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially crafted e-mail message to the user and convincing the user to preview or open the e-mail."* - Microsoft Security Bulletin MS10-064.
- *"The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must click a link listed within an e-mail message."* - Microsoft Security Bulletin MS10-042.
- *"If a user clicks a link in an e-mail message, the user could still be vulnerable to exploitation of this vulnerability through the Web-based attack scenario."* - Microsoft Security Bulletin MS10-053.
- *"The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must open an attachment that is sent in an e-mail message."* - Microsoft Security Bulletin MS10-052.
- *"In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially crafted e-mail message containing an attachment to the user and by convincing the user to open the attachment. When the user attempts to open the attachment, an attacker specified malicious executable file could be run."* - Microsoft Security Bulletin MS10-045.
- *"An attacker could exploit this vulnerability by setting up a malicious e-mail server and convincing the client to connect to this machine."* - Microsoft Security Bulletin MS10-030.
- *"An attacker could host a specially crafted XYZ server that is designed to exploit this vulnerability and then convince a user to initiate an XYZ connection with it. Additionally, an attacker on the local network could perform a man-in-the-middle attack to respond to a legitimate XYZ request with a malformed XYZ response."* - Adapted from Microsoft Security Bulletins MS10-020 and MS10-066.
- *"This vulnerability requires that a user view a specially crafted XYZ file with an affected application."* - Adapted from Microsoft Security Bulletin MS10-043.
- *"This vulnerability requires a user to open a specially crafted XYZ file for any malicious action to occur."* - Adapted from Microsoft Security Bulletin MS10-033.

- *"Exploitation of this vulnerability requires that a user, Windows feature, or application run or install a specially crafted XYZ file."* - Adapted from Microsoft Security Bulletin MS10-019.
- *"An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users."* - Microsoft Security Bulletin MS10-059.
- *"An attacker must have valid logon credentials and be able to log on locally or remotely to exploit this vulnerability."* - Microsoft Security Bulletin MS10-069.
- *"To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and..."* - Microsoft Security Bulletin MS10-059.
- *"By default, printers are not shared on any of the currently supported Windows operating systems. Systems are only vulnerable to remote attack when sharing a printer and the remote attacker can access the printer share."* - Microsoft Security Bulletin MS10-061.

2.3. Identifying The Security Updates For Windows That Resolve Windows Vulnerabilities That Do Not Require User Interaction To Be Exploited

One of the steps in securing a clean installation of Windows is to install the Security Updates for Windows released after the latest Windows Service Pack that resolve Windows vulnerabilities that do not require user interaction to be exploited. To do this, it is necessary to identify the Security Updates for Windows that resolve Windows vulnerabilities that require, or do not require user interaction to be exploited. The following language examples from Microsoft Security Bulletins identify Security Updates for Windows that resolve Windows vulnerabilities that do not require user interaction to be exploited:

- *"Any Windows system connected to a network or the Internet would be at risk."* - Microsoft Security Bulletin MS08-037.
- *"On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit."* - Microsoft Security Bulletin MS08-067.
- *"On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, any anonymous user with access to the target network could deliver a specially crafted network packet to the affected system in order to exploit this vulnerability."* - Microsoft Security Bulletin MS08-067.
- *"An anonymous attacker could exploit the vulnerability by sending specially crafted TCP/IP packets to a computer that has a service listening over the network."* - Microsoft Security Bulletin MS09-048.
- *"An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service."* - Microsoft Security Bulletin MS09-050.
- *"Only attackers on the local subnet would be able to exploit this vulnerability without interaction."* - Microsoft Security Bulletin MS09-063.

3. Preparing For Securing A Clean Installation Of Windows XP/Vista/7

3.1. Preparing For Securing A Clean Installation Of Windows XP

Using a computer that is not compromised, download and copy the following to CD/DVD:

1. The Windows XP Service Packs that bring your installation of Windows XP to Windows XP Service Pack 3:
 - If your Windows product DVD is Windows XP Original Release:
 1. Windows XP Service Pack 2:
 - [Windows XP Service Pack 2 Network Installation Package For IT Professionals And Developers \(microsoft.com\)](http://microsoft.com).
 2. Windows XP Service Pack 3:
 - [Windows XP Service Pack 3 Network Installation Package For IT Professionals And Developers \(microsoft.com\)](http://microsoft.com).
 - If your Windows product DVD is Windows XP Includes Service Pack 1 or Windows XP Includes Service Pack 2:
 1. Windows XP Service Pack 3:
 - [Windows XP Service Pack 3 Network Installation Package For IT Professionals And Developers \(microsoft.com\)](http://microsoft.com).
2. The Security Updates for Windows XP released after Windows XP Service Pack 3 that resolve Windows XP vulnerabilities that do not require user interaction to be exploited:



- The following are through the Microsoft Security Bulletin Summary for May 2012, which includes through MS12-035.
- Supersedece for Microsoft Security Bulletins that resolve SMB vulnerabilities that do and do not require user interaction to be exploited is becoming muddled, even for Microsoft, which has been recently reporting supersedece differently in Microsoft Security Bulletins and Microsoft Security Bulletin Search results. Therefore, rather than guessing on supersedece and possibly omitting Microsoft Security Bulletins that resolve SMB vulnerabilities that do not require user interaction to be exploited, a conservative approach of listing all recent Microsoft Security Bulletins that resolve SMB vulnerabilities that do and do not require user interaction to be exploited is being adopted where deemed necessary.

! Microsoft Security Bulletin MS09-048 describes vulnerabilities in Windows XP Service Pack 2 and Windows XP Service Pack 3 but does not include a Security Update for Windows to resolve them because: "By default, Windows XP Service Pack 2, Windows XP Service Pack 3, and Windows XP Professional x64 Edition Service Pack 2 do not have a listening service configured in the client firewall and are therefore not affected by this vulnerability. Windows XP Service Pack 2 and later operating systems include a stateful host firewall that provides protection for computers against incoming traffic from the Internet or from neighboring network devices on a private network." In other words, the vulnerabilities in Windows XP Service Pack 2 and Windows XP Service Pack 3 described in Microsoft Security Bulletin MS09-048 are not resolved. For additional information, see [Microsoft Security Bulletin MS09-048: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution \(967723\) \(technet.microsoft.com\)](#).

1. [Microsoft Security Bulletin MS08-067 - Critical: Vulnerability In Server Service Could Allow Remote Code Execution \(958644\) \(technet.microsoft.com\)](#):
 - [Security Update For Windows XP \(KB958644\) \(microsoft.com\)](#).
2. [Microsoft Security Bulletin MS09-013 - Critical: Vulnerabilities In Windows HTTP Services Could Allow Remote Code Execution \(960803\) \(technet.microsoft.com\)](#):
 - [Security Update For Windows XP \(KB960803\) \(microsoft.com\)](#).
3. [Microsoft Security Bulletin MS10-029 - Moderate: Vulnerability In Windows ISATAP Component Could Allow Spoofing \(978338\) \(technet.microsoft.com\)](#):
 - [Security Update For Windows XP \(KB978338\) \(microsoft.com\)](#).
4. [Microsoft Security Bulletin MS11-019 - Critical: Vulnerabilities In SMB Client Could Allow Remote Code Execution \(2511455\) \(technet.microsoft.com\)](#):
 - [Security Update For Windows XP \(KB2511455\) \(microsoft.com\)](#).
5. [Microsoft Security Bulletin MS11-020 - Critical: Vulnerability In SMB Server Could Allow Remote Code Execution \(2508429\) \(technet.microsoft.com\)](#):
 - [Security Update For Windows XP \(KB2508429\) \(microsoft.com\)](#).
6. [Microsoft Security Bulletin MS11-030 - Critical: Vulnerability In DNS Resolution Could Allow Remote Code Execution \(2509553\) \(technet.microsoft.com\)](#):
 - [Security Update For Windows XP \(KB2509553\) \(microsoft.com\)](#).
7. [Microsoft Security Bulletin MS11-042 - Critical: Vulnerabilities In Distributed File System Could Allow Remote Code Execution \(2535512\) \(technet.microsoft.com\)](#):
 - [Security Update For Windows XP \(KB2535512\) \(microsoft.com\)](#).
8. [Microsoft Security Bulletin MS11-043 - Critical: Vulnerability In SMB Client Could Allow Remote Code Execution \(2536276\) \(technet.microsoft.com\)](#):

! On August 9, 2011 Microsoft re-released Microsoft Security Bulletin MS11-043 as V2.0 to provide a new version of the Security Update file, itself. The new version of the Security Update file for MS11-043 includes "v2" in the filename. Therefore, if previously downloaded and copied to CD/DVD, replace the original version of the Security Update file for MS11-043 with the v2 version. For additional information, see [Microsoft Security Bulletin MS11-043 - Critical: Vulnerability In SMB Client Could Allow Remote Code Execution \(2536276\) \(technet.microsoft.com\)](#).

- [Security Update For Windows XP \(KB2536276\) \(microsoft.com\)](#).
3. If not installed by Windows XP or located on a disc included with your computer, the Windows XP driver for your network device (i.e., dial-up modem or ethernet adapter).

3.2. Preparing For Securing A Clean Installation Of Windows Vista

Using a computer that is not compromised, download and copy the following to CD/DVD:

1. The Windows Vista Service Packs that bring your installation of Windows Vista to Windows Vista Service Pack 2:
 - If your Windows product DVD is Windows Vista Original Release:
 1. Windows Vista Service Pack 1:
 - 32-bit: [Windows Vista Service Pack 1 All Language Standalone \(KB936330\) \(microsoft.com\)](#).
 - 64-bit: [Windows Vista Service Pack 1 All Language Standalone For x64-Based Systems \(KB936330\) \(microsoft.com\)](#).
 2. Windows Vista Service Pack 2:
 - 32-bit: [Windows Server 2008 Service Pack 2 And Windows Vista Service Pack 2 - All Language Standalone \(KB948465\) \(microsoft.com\)](#).
 - 64-bit: [Windows Server 2008 Service Pack 2 And Windows Vista Service Pack 2 - All Language Standalone For x64-Based Systems \(KB948465\) \(microsoft.com\)](#).

- If your Windows product DVD is Windows Vista Includes Service Pack 1:

1. Windows Vista Service Pack 2:

- 32-bit: [Windows Server 2008 Service Pack 2 And Windows Vista Service Pack 2 - All Language Standalone \(KB948465\) \(microsoft.com\)](#).
- 64-bit: [Windows Server 2008 Service Pack 2 And Windows Vista Service Pack 2 - All Language Standalone For x64-Based Systems \(KB948465\) \(microsoft.com\)](#).

2. The Security Updates for Windows Vista released after Windows Vista Service Pack 2 that resolve Windows Vista vulnerabilities that do not require user interaction to be exploited:



- The following are through the Microsoft Security Bulletin Summary for May 2012, which includes through MS12-035.
- Supersedece for Microsoft Security Bulletins that resolve SMB vulnerabilities that do and do not require user interaction to be exploited is becoming muddled, even for Microsoft, which has been recently reporting supersedece differently in Microsoft Security Bulletins and Microsoft Security Bulletin Search results. Therefore, rather than guessing on supersedece and possibly omitting Microsoft Security Bulletins that resolve SMB vulnerabilities that do not require user interaction to be exploited, a conservative approach of listing all recent Microsoft Security Bulletins that resolve SMB vulnerabilities that do and do not require user interaction to be exploited is being adopted where deemed necessary.

1. [Microsoft Security Bulletin MS09-048 - Critical: Vulnerabilities In Windows TCP/IP Could Allow Remote Code Execution \(967723\) \(technet.microsoft.com\)](#):
 - 32-bit: [Security Update For Windows Vista \(KB967723\) \(microsoft.com\)](#).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB967723\) \(microsoft.com\)](#).
2. [Microsoft Security Bulletin MS09-063 - Critical: Vulnerability In Web Services On Devices API Could Allow Remote Code Execution \(973565\) \(technet.microsoft.com\)](#):
 - 32-bit: [Security Update For Windows Vista \(KB973565\) \(microsoft.com\)](#).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB973565\) \(microsoft.com\)](#).
3. [Microsoft Security Bulletin MS10-029 - Moderate: Vulnerability In Windows ISATAP Component Could Allow Spoofing \(978338\) \(technet.microsoft.com\)](#):



On March 13, 2012 Microsoft re-released Microsoft Security Bulletin MS10-058 as V2.0 to report that MS10-029 is not replaced by MS10-058 on Windows Vista as previously reported. Since MS10-029 is not replaced by MS10-054, which is replaced by MS11-064, which is replaced by MS11-083, which is included in this list, and since MS10-029 is a Security Update for Windows Vista released after Windows Vista Service Pack 2 that resolves Windows Vista vulnerabilities that do not require user interaction to be exploited, MS10-029 was re-added to this list on March 15, 2012. For additional information, see [Microsoft Security Bulletin MS10-058 - Important: Vulnerabilities In TCP/IP Could Allow Elevation Of Privilege \(978886\) \(technet.microsoft.com\)](#).

- 32-bit: [Security Update For Windows Vista \(KB978338\) \(microsoft.com\)](#).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB978338\) \(microsoft.com\)](#).
4. [Microsoft Security Bulletin MS11-019 - Critical: Vulnerabilities In SMB Client Could Allow Remote Code Execution \(2511455\) \(technet.microsoft.com\)](#):
 - 32-bit: [Security Update For Windows Vista \(KB2511455\) \(microsoft.com\)](#).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB2511455\) \(microsoft.com\)](#).
 5. [Microsoft Security Bulletin MS11-020 - Critical: Vulnerability In SMB Server Could Allow Remote Code Execution \(2508429\) \(technet.microsoft.com\)](#):
 - 32-bit: [Security Update For Windows Vista \(KB2508429\) \(microsoft.com\)](#).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB2508429\) \(microsoft.com\)](#).
 6. [Microsoft Security Bulletin MS11-030 - Critical: Vulnerability In DNS Resolution Could Allow Remote Code Execution \(2509553\) \(technet.microsoft.com\)](#):
 - 32-bit: [Security Update For Windows Vista \(KB2509553\) \(microsoft.com\)](#).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB2509553\) \(microsoft.com\)](#).
 7. [Microsoft Security Bulletin MS11-042 - Critical: Vulnerabilities In Distributed File System Could Allow Remote Code Execution \(2535512\) \(technet.microsoft.com\)](#):
 - 32-bit: [Security Update For Windows Vista \(KB2535512\) \(microsoft.com\)](#).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB2535512\) \(microsoft.com\)](#).
 8. [Microsoft Security Bulletin MS11-043 - Critical: Vulnerability In SMB Client Could Allow Remote Code Execution \(2536276\) \(technet.microsoft.com\)](#):



On August 9, 2011 Microsoft re-released Microsoft Security Bulletin MS11-043 as V2.0 to provide a new version of the Security Update file, itself. The new version of the Security Update file for MS11-043 includes "v2" in the filename. Therefore, if previously downloaded and copied to CD/DVD, replace the original version of the Security Update file for MS11-043 with the v2 version. For additional information, see [Microsoft Security](#)

Bulletin MS11-043 - Critical: Vulnerability In SMB Client Could Allow Remote Code Execution (2536276) (technet.microsoft.com).

- 32-bit: [Security Update For Windows Vista \(KB2536276\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB2536276\) \(microsoft.com\)](http://microsoft.com).
9. [Microsoft Security Bulletin MS11-048 - Important: Vulnerability In SMB Server Could Allow Denial Of Service \(2536275\) \(technet.microsoft.com\)](http://technet.microsoft.com):
 - 32-bit: [Security Update For Windows Vista \(KB2536275\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB2536275\) \(microsoft.com\)](http://microsoft.com).
 10. [Microsoft Security Bulletin MS11-053 - Critical: Vulnerability In Bluetooth Stack Could Allow Remote Code Execution \(2566220\) \(technet.microsoft.com\)](http://technet.microsoft.com):
 - 32-bit: [Security Update For Windows Vista \(KB2532531\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB2532531\) \(microsoft.com\)](http://microsoft.com).
 11. [Microsoft Security Bulletin MS12-032 - Important: Vulnerability In TCP/IP Could Allow Elevation Of Privilege \(2688338\) \(technet.microsoft.com\)](http://technet.microsoft.com):
 - 32-bit: [Security Update For Windows Vista \(KB2688338\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows Vista For x64-Based Systems \(KB2688338\) \(microsoft.com\)](http://microsoft.com).
3. If not installed by Windows Vista or located on a disc included with your computer, the Windows Vista driver for your network device (i.e., dial-up modem or ethernet adapter).

3.3. Preparing For Securing A Clean Installation Of Windows 7

Using a computer that is not compromised, download and copy the following to CD/DVD:

1. The Windows 7 Service Packs that bring your installation of Windows 7 to Windows 7 Service Pack 1:
 - If your Windows product DVD is Windows 7 Original Release:
 1. Windows 7 Service Pack 1:
 - 32-bit: The file, windows6.1-KB976932-X86.exe, at [Windows 7 And Windows Server 2008 R2 Service Pack 1 \(KB976932\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: The file, windows6.1-KB976932-X64.exe, at [Windows 7 And Windows Server 2008 R2 Service Pack 1 \(KB976932\) \(microsoft.com\)](http://microsoft.com).
2. The Security Updates for Windows 7 released after Windows 7 Service Pack 1 that resolve Windows 7 vulnerabilities that do not require user interaction to be exploited:

i

- The following are through the Microsoft Security Bulletin Summary for May 2012, which includes through MS12-035.
- Supersedece for Microsoft Security Bulletins that resolve SMB vulnerabilities that do and do not require user interaction to be exploited is becoming muddled, even for Microsoft, which has been recently reporting supersedece differently in Microsoft Security Bulletins and Microsoft Security Bulletin Search results. Therefore, rather than guessing on supersedece and possibly omitting Microsoft Security Bulletins that resolve SMB vulnerabilities that do not require user interaction to be exploited, a conservative approach of listing all recent Microsoft Security Bulletins that resolve SMB vulnerabilities that do and do not require user interaction to be exploited is being adopted where deemed necessary.

1. [Microsoft Security Bulletin MS11-019 - Critical: Vulnerabilities In SMB Client Could Allow Remote Code Execution \(2511455\) \(technet.microsoft.com\)](http://technet.microsoft.com):
 - 32-bit: [Security Update For Windows 7 \(KB2511455\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows 7 For x64-Based Systems \(KB2511455\) \(microsoft.com\)](http://microsoft.com).
2. [Microsoft Security Bulletin MS11-020 - Critical: Vulnerability In SMB Server Could Allow Remote Code Execution \(2508429\) \(technet.microsoft.com\)](http://technet.microsoft.com):
 - 32-bit: [Security Update For Windows 7 \(KB2508429\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows 7 For x64-Based Systems \(KB2508429\) \(microsoft.com\)](http://microsoft.com).
3. [Microsoft Security Bulletin MS11-030 - Critical: Vulnerability In DNS Resolution Could Allow Remote Code Execution \(2509553\) \(technet.microsoft.com\)](http://technet.microsoft.com):
 - 32-bit: [Security Update For Windows 7 \(KB2509553\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows 7 For x64-Based Systems \(KB2509553\) \(microsoft.com\)](http://microsoft.com).
4. [Microsoft Security Bulletin MS11-043 - Critical: Vulnerability In SMB Client Could Allow Remote Code Execution \(2536276\) \(technet.microsoft.com\)](http://technet.microsoft.com):

!

On August 9, 2011 Microsoft re-released Microsoft Security Bulletin MS11-043 as V2.0 to provide a new version of the Security Update file, itself. The new version of the Security Update file for MS11-043 includes "v2" in the filename. Therefore, if previously downloaded and copied to CD/DVD, replace the original version of the Security Update file for MS11-043 with the v2 version. For additional information, see [Microsoft Security](http://microsoft.com)

Bulletin MS11-043 - Critical: Vulnerability In SMB Client Could Allow Remote Code Execution (2536276) (technet.microsoft.com).

- 32-bit: [Security Update For Windows 7 \(KB2536276\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows 7 For x64-Based Systems \(KB2536276\) \(microsoft.com\)](http://microsoft.com).
5. [Microsoft Security Bulletin MS11-048 - Important: Vulnerability In SMB Server Could Allow Denial Of Service \(2536275\) \(technet.microsoft.com\)](http://technet.microsoft.com):
 - 32-bit: [Security Update For Windows 7 \(KB2536275\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows 7 For x64-Based Systems \(KB2536275\) \(microsoft.com\)](http://microsoft.com).
 6. [Microsoft Security Bulletin MS11-053 - Critical: Vulnerability In Bluetooth Stack Could Allow Remote Code Execution \(2566220\) \(technet.microsoft.com\)](http://technet.microsoft.com):
 - 32-bit: [Security Update For Windows 7 \(KB2532531\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows 7 For x64-Based Systems \(KB2532531\) \(microsoft.com\)](http://microsoft.com).
 7. [Microsoft Security Bulletin MS12-032 - Important: Vulnerability In TCP/IP Could Allow Elevation Of Privilege \(2688338\) \(technet.microsoft.com\)](http://technet.microsoft.com):
 - 32-bit: [Security Update For Windows 7 \(KB2688338\) \(microsoft.com\)](http://microsoft.com).
 - 64-bit: [Security Update For Windows 7 For x64-Based Systems \(KB2688338\) \(microsoft.com\)](http://microsoft.com).
3. If not installed by Windows 7 or located on a disc included with your computer, the Windows 7 driver for your network device (i.e., dial-up modem or ethernet adapter).

4. Securing A Clean Installation Of Windows XP/Vista/7

4.1. Securing A Clean Installation Of Windows XP

1. Perform the following offline, and before interacting with the computer in a way that could result in compromise:
 1. A clean, default installation of Windows XP:
 1. Boot the computer from the Windows XP product CD.
 2. In Windows XP Setup:
 - If the hard disk is new, create a new partition for the installation of Windows XP.
 - If the hard disk already contains Windows, delete the Windows partition, delete any other partitions you want to delete, and create a new partition for the installation of Windows XP.
 3. Otherwise, select **default/typical/recommended** throughout.
 2. As previously downloaded and copied to CD/DVD, install the Windows XP Service Packs that bring your installation of Windows XP to Windows XP Service Pack 3:
 - If you installed Windows XP Original Release:
 1. Windows XP Service Pack 2.
 2. Windows XP Service Pack 3.
 - If you installed Windows XP Includes Service Pack 1 or Windows XP Includes Service Pack 2:
 1. Windows XP Service Pack 3.
 3. As previously downloaded and copied to CD/DVD, install the Security Updates for Windows XP released after Windows XP Service Pack 3 that resolve Windows XP vulnerabilities that do not require user interaction to be exploited:



It is not necessary to restart the computer after installing each Security Update for Windows. Therefore, if prompted to restart the computer after installing a Security Update for Windows, you can wait and restart the computer after installing the last Security Update for Windows.

1. Microsoft Security Bulletin MS08-067 - Critical: Vulnerability In Server Service Could Allow Remote Code Execution (958644).
2. Microsoft Security Bulletin MS09-013 - Critical: Vulnerabilities In Windows HTTP Services Could Allow Remote Code Execution (960803).
3. Microsoft Security Bulletin MS10-029 - Moderate: Vulnerability In Windows ISATAP Component Could Allow Spoofing (978338).
4. Microsoft Security Bulletin MS11-019 - Critical: Vulnerabilities In SMB Client Could Allow Remote Code Execution (2511455).
5. Microsoft Security Bulletin MS11-020 - Critical: Vulnerability In SMB Server Could Allow Remote Code Execution (2508429).
6. Microsoft Security Bulletin MS11-030 - Critical: Vulnerability In DNS Resolution Could Allow Remote Code Execution (2509553).
7. Microsoft Security Bulletin MS11-042 - Critical: Vulnerabilities In Distributed File System Could Allow Remote Code Execution (2535512).
8. Microsoft Security Bulletin MS11-043 - Critical: Vulnerability In SMB Client Could Allow Remote Code Execution (2536276).

4. If not installed by Windows XP, as located on a disc included with your computer or as previously downloaded and copied to CD/DVD, install the Windows XP driver for your network device (i.e., dial-up modem or ethernet adapter).
 5. Install your anti-virus/firewall software.
2. Perform the following online, and before interacting with the computer in a way that could result in compromise:
 1. Run Windows/Microsoft Update and install the Security Updates for Windows.
 2. Run Windows/Microsoft Update and install the other available updates.
 3. Install the updates for your anti-virus/firewall software and perform a full system scan to confirm your computer is not compromised.
 3. You have secured a clean installation of Windows XP. If you use imaging software such as Acronis True Image or Norton Ghost, this is an excellent time to image your system. Otherwise, you may proceed to use your computer as normal.

4.2. Securing A Clean Installation Of Windows Vista

1. Perform the following offline, and before interacting with the computer in a way that could result in compromise:
 1. A clean, default installation of Windows Vista:
 1. Boot the computer from the Windows Vista product DVD.
 2. When the Install Windows: Which type of installation do you want dialog appears, click **Custom (advanced)**.
 3. When the Install Windows: Where do you want to install Windows dialog appears:
 - If the hard disk is new, create a new partition for the installation of Windows Vista.
 - If the hard disk already contains Windows, delete the Windows partition, delete any other partitions you want to delete, and create a new partition for the installation of Windows Vista.
 4. Otherwise, select **default/typical/recommended** throughout.
 2. As previously downloaded and copied to CD/DVD, install the Windows Vista Service Packs that bring your installation of Windows Vista to Windows Vista Service Pack 2:
 - If you installed Windows Vista Original Release:
 1. Windows Vista Service Pack 1.
 2. Windows Vista Service Pack 2.
 - If you installed Windows Vista Includes Service Pack 1:
 1. Windows Vista Service Pack 2.
 3. As previously downloaded and copied to CD/DVD, install the Security Updates for Windows Vista released after Windows Vista Service Pack 2 that resolve Windows Vista vulnerabilities that do not require user interaction to be exploited:



It is not necessary to restart the computer after installing each Security Update for Windows. Therefore, if prompted to restart the computer after installing a Security Update for Windows, you can wait and restart the computer after installing the last Security Update for Windows.

1. Microsoft Security Bulletin MS09-048 - Critical: Vulnerabilities In Windows TCP/IP Could Allow Remote Code Execution (967723).
 2. Microsoft Security Bulletin MS09-063 - Critical: Vulnerability In Web Services On Devices API Could Allow Remote Code Execution (973565).
 3. Microsoft Security Bulletin MS10-029 - Moderate: Vulnerability In Windows ISATAP Component Could Allow Spoofing (978338).
 4. Microsoft Security Bulletin MS11-019 - Critical: Vulnerabilities In SMB Client Could Allow Remote Code Execution (2511455).
 5. Microsoft Security Bulletin MS11-020 - Critical: Vulnerability In SMB Server Could Allow Remote Code Execution (2508429).
 6. Microsoft Security Bulletin MS11-030 - Critical: Vulnerability In DNS Resolution Could Allow Remote Code Execution (2509553).
 7. Microsoft Security Bulletin MS11-042 - Critical: Vulnerabilities In Distributed File System Could Allow Remote Code Execution (2535512).
 8. Microsoft Security Bulletin MS11-043 - Critical: Vulnerability In SMB Client Could Allow Remote Code Execution (2536276).
 9. Microsoft Security Bulletin MS11-048 - Important: Vulnerability In SMB Server Could Allow Denial Of Service (2536275).
 10. Microsoft Security Bulletin MS11-053 - Critical: Vulnerability In Bluetooth Stack Could Allow Remote Code Execution (2566220).
 11. Microsoft Security Bulletin MS12-032 - Important: Vulnerability In TCP/IP Could Allow Elevation Of Privilege (2688338).
4. If not installed by Windows Vista, as located on a disc included with your computer or as previously downloaded and copied to CD/DVD, install the Windows Vista driver for your network device (i.e., dial-up modem or ethernet adapter).
 5. Install your anti-virus/firewall software.
2. Perform the following online, and before interacting with the computer in a way that could result in compromise:

1. Run Windows/Microsoft Update and install the Security Updates for Windows.
 2. Run Windows/Microsoft Update and install the other available updates.
 3. Install the updates for your anti-virus/firewall software and perform a full system scan to confirm your computer is not compromised.
3. You have secured a clean installation of Windows Vista. If you use imaging software such as Acronis True Image or Norton Ghost, this is an excellent time to image your system. Otherwise, you may proceed to use your computer as normal.

4.3. Securing A Clean Installation Of Windows 7

1. Perform the following offline, and before interacting with the computer in a way that could result in compromise:
 1. A clean, default installation of Windows 7:
 1. Boot the computer from the Windows 7 product DVD.
 2. When the Install Windows: Which type of installation do you want dialog appears, click **Custom (advanced)**.
 3. When the Install Windows: Where do you want to install Windows dialog appears:
 - If the hard disk is new, create a new partition for the installation of Windows 7.
 - If the hard disk already contains Windows, delete the Windows partition, delete any other partitions you want to delete, and create a new partition for the installation of Windows 7.
 4. Otherwise, select **default/typical/recommended** throughout.
 2. As previously downloaded and copied to CD/DVD, install the Windows 7 Service Packs that bring your installation of Windows 7 to Windows 7 Service Pack 1:
 - If you installed Windows 7 Original Release:
 1. Windows 7 Service Pack 1.
 3. As previously downloaded and copied to CD/DVD, install the Security Updates for Windows 7 released after Windows 7 Service Pack 1 that resolve Windows 7 vulnerabilities that do not require user interaction to be exploited:



It is not necessary to restart the computer after installing each Security Update for Windows. Therefore, if prompted to restart the computer after installing a Security Update for Windows, you can wait and restart the computer after installing the last Security Update for Windows.

1. Microsoft Security Bulletin MS11-019 - Critical: Vulnerabilities In SMB Client Could Allow Remote Code Execution (2511455).
 2. Microsoft Security Bulletin MS11-020 - Critical: Vulnerability In SMB Server Could Allow Remote Code Execution (2508429).
 3. Microsoft Security Bulletin MS11-030 - Critical: Vulnerability In DNS Resolution Could Allow Remote Code Execution (2509553).
 4. Microsoft Security Bulletin MS11-043 - Critical: Vulnerability In SMB Client Could Allow Remote Code Execution (2536276).
 5. Microsoft Security Bulletin MS11-048 - Important: Vulnerability In SMB Server Could Allow Denial Of Service (2536275).
 6. Microsoft Security Bulletin MS11-053 - Critical: Vulnerability In Bluetooth Stack Could Allow Remote Code Execution (2566220).
 7. Microsoft Security Bulletin MS12-032 - Important: Vulnerability In TCP/IP Could Allow Elevation Of Privilege (2688338).
4. If not installed by Windows 7, as located on a disc included with your computer or as previously downloaded and copied to CD/DVD, install the Windows 7 driver for your network device (i.e., dial-up modem or ethernet adapter).
 5. Install your anti-virus/firewall software.
2. Perform the following online, and before interacting with the computer in a way that could result in compromise:
 1. Run Windows/Microsoft Update and install the Security Updates for Windows.
 2. Run Windows/Microsoft Update and install the other available updates.
 3. Install the updates for your anti-virus/firewall software and perform a full system scan to confirm your computer is not compromised.
 3. You have secured a clean installation of Windows 7. If you use imaging software such as Acronis True Image or Norton Ghost, this is an excellent time to image your system. Otherwise, you may proceed to use your computer as normal.

5. Additional Reading

- [Description Of The Standard Terminology That Is Used To Describe Microsoft Software Updates \(824684\) \(support.microsoft.com\)](http://support.microsoft.com/kb/824684)
- [Update Management Process \(technet.microsoft.com\)](http://technet.microsoft.com)
- [How To Obtain The Latest Windows XP Service Pack \(322389\) \(support.microsoft.com\)](http://support.microsoft.com/kb/322389)
- [List Of Fixes In Windows XP Service Pack 1 And Windows XP Service Pack 1a \(324720\) \(support.microsoft.com\)](http://support.microsoft.com/kb/324720)
- [Differences Between Windows XP SP1 And Windows XP SP1a \(813926\) \(support.microsoft.com\)](http://support.microsoft.com/kb/813926)
- [Windows XP Service Pack 2 Network Installation Package For IT Professionals And Developers \(microsoft.com\)](http://microsoft.com)
- [Release Notes For Windows XP Service Pack 2 \(835935\) \(support.microsoft.com\)](http://support.microsoft.com/kb/835935)

- [List Of Fixes Included In Windows XP Service Pack 2 \(811113\) \(support.microsoft.com\)](#)
- [Security Bulletins Included In Windows XP Service Pack 2 \(technet.microsoft.com\)](#)
- [Windows XP Service Pack 3 Network Installation Package For IT Professionals And Developers \(microsoft.com\)](#)
- [List Of Fixes That Are Included In Windows XP Service Pack 3 \(946480\) \(support.microsoft.com\)](#)
- [General Information Regarding Windows Server 2003 Service Pack 2 \(914961\) \(support.microsoft.com\)](#)
- [A Description Of The x64-Based Versions Of Windows Server 2003 And Of Windows XP Professional x64 Edition \(888733\) \(support.microsoft.com\)](#)
- [Information About Windows XP Service Pack 3 \(936929\) \(support.microsoft.com\)](#)
- [How To Obtain The Latest Windows Vista Service Pack \(935791\) \(support.microsoft.com\)](#)
- [Windows Vista Service Pack 1 All Language Standalone \(KB936330\) \(microsoft.com\)](#)
- [Windows Vista Service Pack 1 All Language Standalone For x64-Based Systems \(KB936330\) \(microsoft.com\)](#)
- [Hotfixes And Security Updates Included In Windows Vista Service Pack 1 \(technet2.microsoft.com\)](#)
- [Windows Server 2008 Service Pack 2 And Windows Vista Service Pack 2 - All Language Standalone \(KB948465\) \(microsoft.com\)](#)
- [Windows Server 2008 Service Pack 2 and Windows Vista Service Pack 2 - All Language Standalone For x64-based Systems \(KB948465\) \(microsoft.com\)](#)
- [Hotfixes And Security Updates In Windows Server 2008 SP2 And Windows Vista SP2 \(technet.microsoft.com\)](#)
- [Windows 7 And Windows Server 2008 R2 Service Pack 1 \(KB976932\) \(microsoft.com\)](#)
- [Documentation For Windows 7 And Windows Server 2008 R2 Service Pack 1 \(KB976932\) \(microsoft.com\)](#)

Steve's Tech Resource

The Web Development, Internet, Software, Hardware, and Multimedia Resource



Copyright © 2000-2012 Steve's Tech Resource