Microsoft Security Update Guide

Second Edition

Helping IT Professionals Better Understand and Maximize Microsoft Security Update Release Information, Processes, Communications and Tools
Contents
Welcome .......................................................................................................................... 1
How to Use the Microsoft Security Update Guide...................................................... 2
Introduction .................................................................................................................... 2
Managing Vulnerabilities ............................................................................................. 6
   Purpose of this Guide ................................................................................................. 6
   Vulnerability Management at Microsoft ................................................................. 7
Managing Security Updates by Using Microsoft Solutions ........................................... 9
   Three Approaches to Security Updates .................................................................. 10
The Microsoft Security Update Release Process ....................................................... 15
   How Microsoft Tests Security Updates .................................................................. 16
   Application Compatibility Testing ........................................................................ 17
   Rootkit Detection .................................................................................................... 18
   Security Test Pass .................................................................................................... 18
   Security Update Validation Program ..................................................................... 19
Microsoft Security Release Communications ............................................................ 19
   Security Bulletin Advance Notification ................................................................ 19
   Security Bulletin Summary ...................................................................................... 20
   Security Bulletin ..................................................................................................... 20
   Security Update ...................................................................................................... 20
   Knowledge Base (KB) Articles .............................................................................. 21
   Security Advisory ................................................................................................... 21
   Predictable Security Update Release Process .................................................... 21
Fraudulent Notifications That Target Microsoft Security Updates ................................ 23
Customer Risk Management Framework ..................................................................... 23
Stage 1: Receive Microsoft Security Release Communications .................. 25

Microsoft Security Release Communications ...................................... 25
Receiving Microsoft Security Release Communications ....................... 26

Stage 2: Evaluate Risk ........................................................................... 28

Determinations in the Risk Management Framework ............................. 30
Does Your Organization Lack an Existing Risk Management Process? ...... 31
Identify Whether the Vulnerability Applies .......................................... 31
Gathering Security Vulnerability Intelligence ......................................... 32
Determining the Vulnerability Risk ....................................................... 35
The Microsoft Severity Rating System .................................................. 36
Risk Evaluation Resources ................................................................. 38
Example: Applying Microsoft Guidance to Evaluate Risk ....................... 46
Example: Applying Intelligence to Determine Risk Rating ....................... 47
Security Update Deployment Considerations ......................................... 48

Stage 3: Evaluate Mitigation .................................................................. 54

A Viable Short-Term Security Control ................................................... 55

Stage 4: Deploy Updates ....................................................................... 59

The Deploying Microsoft Windows Server Update Services Guide .......... 62
Standard and Urgent Deployments ......................................................... 62
Standard Package Application Process ............................................... 62
Planning the Deployment .................................................................... 63
Example: Planning Security Update Deployment ..................................... 64
Is a Security Update Available for Download? ....................................... 66
Obtaining the Required Security Update Files from a Trusted Source ........ 67
Creating Update Packages .................................................................. 68
Testing Update Packages .................................................................... 70
Test Environment.................................................................70
Pilot Deployment.................................................................72
Test Process Steps...............................................................72
Deploying Update Packages..................................................83
Submitting a Change Request...............................................86
Communicating the Rollout Schedule to the Organization........86
Installing the Update............................................................87
Accelerating Security Update Deployment...............................89
Creating Update Packages....................................................89
Testing Packages....................................................................89
Deploying Packages..............................................................89
Stage 5: Monitor Systems.......................................................90
Successful Update Deployment..............................................91
Confirming Update Installation..............................................92
Uninstalling Security Updates...............................................94
Post-Implementation Review................................................96
Short-Term Mitigation Removal............................................96
Stage 6: Use Microsoft Resources to Track Security Developments.........97
Major and Minor Security Bulletin and Advisory Revisions........98
The Constant Threat from Malicious Software........................99
Other Security Resources.....................................................101
Summary..............................................................................102
Feedback...............................................................................102
Appendix..............................................................................104
The Microsoft Security Update Release and Deployment Process Diagram104
Microsoft Security Update Terminology................................106
Microsoft Security Updates ................................................................. 107
Windows Update or Microsoft Update? ............................................... 109
Security Update Policy for Non-Genuine Software............................... 110
Glossary and Commonly Used Terms .................................................. 111
Welcome

A Message from Trustworthy Computing Security General Manager, Matt Thomlinson

Welcome to the Microsoft Security Update Guide, Second Edition. Our aim with the Guide is to help you manage the process of deploying Microsoft security updates within your environment. Microsoft produces a lot of information and guidance about our security updates, and the Guide describes how to use these resources effectively to help make your organization’s IT environment secure.

At Microsoft we know that deploying updates can be a time-consuming activity, with pre-deployment testing being a critical part of the process. To help you with this task it is vital that we test our updates extensively before they are released. We create updates for more than a billion systems worldwide, so we have developed extensive processes for testing updates:

- Testing against all supported versions and service packs of the affected software, in all supported languages
- Extensive application compatibility testing including more than 3,000 of the most widely deployed third-party applications
- The Security Update Validation Program (SUVP) which allows selected customers and partners to test an update’s functionality before release
- Internal testing at Microsoft, including live deployment on more than 24,000 devices across the company

Only after an update has passed all of these tests is it approved for release. You will find more detail on these testing processes – and updated guidance on performing testing in your own environment – within this Guide.

I hope you will find the Guide to be a valuable resource of in-depth information and tools that will help you protect your IT infrastructure, and create a safer, more secure computing and Internet environment.

Matt Thomlinson

General Manager, Trustworthy Computing Security

Trustworthy Computing Group
How to Use the Microsoft Security Update Guide

Welcome to the Microsoft® Security Update Guide.

This guide was designed to help IT pros better understand and use Microsoft security release information, processes, communications, and tools. Our goal is to help IT pros understand how Microsoft security updates are developed and tested; manage organizational risk; and develop a repeatable, effective deployment mechanism for testing and releasing security updates.

In this guide, you will find a convenient glossary of terms, an overview of the Microsoft Security Bulletin process, and a stage-by-stage review of Microsoft Security Updates.

The guide is organized according to the following stages of the security update process:

♦ Stage 1: Receive Microsoft Security Release Communications
♦ Stage 2: Evaluate Risk
♦ Stage 3: Evaluate Mitigation
♦ Stage 4: Deploy Standard or Urgent Updates
♦ Stage 5: Monitor Systems
♦ Stage 6: Use Microsoft Resources to Track Security Developments.

Each of these sections outlines the purpose and objective for each stage, as well as the expected target outcomes after completing each stage.

We hope this guide will serve as a valuable resource to help protect your IT infrastructure. Moreover, we hope the guide represents yet another step forward in our broader collaboration as we seek to create a safer, and more secure computing framework in the 21st century.

Introduction

Vulnerabilities are weaknesses in software that may enable an attacker to compromise the integrity, availability, or confidentiality of that software. Some of the worst vulnerabilities enable attackers to run arbitrary code on the compromised system. A vulnerability disclosure is the revelation of the existence of a vulnerability to the public at large. Disclosures can come from various sources, including software vendors, security software vendors, independent security researchers, and even creators of malicious software (malware). Research in the
Security Intelligence Report (SIR)\(^1\) shows thousands of vulnerability disclosures of varying severities across the entire software industry disclosed every half-year from the second half of 2006 to the first half of 2010.

Figure 1: Industry-wide vulnerability disclosures by half-year, 2H06-1H10

Of these vulnerability disclosures, the majority are scored as High or Medium severity vulnerabilities according to the industry standard Common Vulnerability Scoring System (CVSS),\(^2\) while with only a minority are scored as Low severity, as indicated in Figure 2.

---

\(^1\) [www.microsoft.com/sir](http://www.microsoft.com/sir)

\(^2\) See [www.first.org/cvss/cvss-guide.html](http://www.first.org/cvss/cvss-guide.html) for information about the CVSS and its criteria for scoring vulnerability severity and complexity.
The CVSS also scores vulnerabilities by access complexity, which measures how difficult it is for attackers to exploit a given vulnerability. As with vulnerability severity, the picture that emerges as indicated in Figure 3 is not a positive one. In most periods, the majority of vulnerabilities are Low complexity, which means that they can be exploited with relative ease without requiring specialized access conditions.
Vulnerabilities are an industry-wide problem. There are thousands of vulnerability disclosures across the industry each year, affecting software from Microsoft and many other vendors. Figure 4 shows vulnerabilities for Microsoft and non-Microsoft products since 2006.

Managing Security Updates is vital. An exploit is malicious code that takes advantage of software vulnerabilities. The research in the SIR shows that exploits remain active long after the security update for the vulnerability is available because some users install updates only sporadically or not at all. Even today,
exploits for vulnerabilities that were resolved in 2003 still exist. This shows that when attackers understand how to exploit a given vulnerability, despite the existence of a security update for it, they will routinely attempt to use that exploit to compromise “unpatched” systems using various attack methods for years to come. Moreover, in a recent volume of the SIR, Microsoft analyzed a sample of several hundred files in a given period that were used for successful attacks. The research showed there was a finite number of exploits for specific vulnerabilities and that security updates were available for all of the vulnerabilities at the time of attack; the affected users were exposed because they had not applied the updates. Applying new security updates quickly and consistently would have prevented all of these attacks from succeeding on any supported version of the software application.

This is the setting in which enterprise IT administrators and security pros find themselves today. The process of maintaining an organization’s desktop computers, servers, virtual machines, and mobile devices with the latest security updates for the operating system and applications has become a central part of the risk-management methodology for any Internet-connected environment.

Managing Vulnerabilities

This section covers:

- The purpose of this guide.
- How Microsoft manages vulnerabilities in its products.

At the end of this section, IT pros should:

- Understand the purpose of this guide, which is to help IT pros maximize all attendant communications, guidance, programs, and services that Microsoft releases to help manage security vulnerabilities in an organization’s IT environment.

Purpose of this Guide

In an effort to mitigate the threats that online criminal activity poses to businesses, IT pros need to understand the Microsoft security update release process and all supporting resources from Microsoft. In addition to supporting and maintaining the vitality of the IT environment, IT pros should understand how each software vendor’s security communication and security update release process works. This guide helps IT pros plan for and manage the two types of Microsoft security releases — (1) security updates and (2) security advisories — and all of the Microsoft communications, guidance, programs and services related to them. Understanding all of the components and communications that a Microsoft security release contains helps IT pros enhance their security guidance and stay informed. If IT pros cannot determine and maintain a level of trust
within the organization’s operating systems and application software, the organization might risk creating or not addressing a variety of security vulnerabilities. In addition, a lack of such oversight might cause a security breach that could lead to a loss of revenue, costs associated with cleaning up and rebuilding the IT environment, loss of intellectual property, litigation, or worse. Minimizing this threat requires organizations to configure systems properly, use the latest software, and install the recommended security updates. Creating and communicating a documented security release and update policy for any organization is a vital part of any company's risk-management process.

This guide was designed to help IT pros better understand and use Microsoft security release information, processes, communications, and tools. Our goal is to help IT pros manage organizational risk and develop a repeatable, effective deployment mechanism for security updates.

**Risk management framework as a backdrop.** To help IT pros understand how various Microsoft security update release communications, guidance, programs, and services can help their organizations with risk-management, this guide follows a general customer risk-management framework. The framework is shown in Figure 5 and discussed in more detail later. The framework is purposely meant to be general and serve as a baseline for IT pros to follow, but is specific enough to be relevant and help convey where certain Microsoft resources fit throughout a risk-management framework.

**Figure 5. The customer risk management framework**

---

**Vulnerability Management at Microsoft**

**Software vulnerabilities are a fact of life.** Throughout the product software life cycle, from conception to release to deployment and thereafter, it is impossible to prevent all vulnerabilities. The Microsoft Security Development Lifecycle (SDL)\(^3\) is intended to reduce the number of vulnerabilities in Microsoft software in addition to reducing the severity and impact of those that remain. Because

---

\(^3\) www.microsoft.com/sdl
software is developed by humans, some vulnerabilities do remain in software code. To help better protect customers, the Microsoft Trustworthy Computing (TwC) group includes the Microsoft Security Response Center (MSRC)\(^4\) — the center that investigates potential and existing vulnerabilities in Microsoft software.

Microsoft understands that security vulnerabilities in Microsoft products have the potential to disrupt customer experiences. To help protect customers from potential disruptive behavior by criminals seeking to gain access to systems and information through a cyber-attack, Microsoft has developed a security update release process that seeks to give customers a high level of consistency, predictability, quality, and transparency while minimizing risk. The goal is to make it easier for customers to understand the related risks to their IT environment, enabling them to plan, resource, schedule and budget for the associated system maintenance. This security update release process has evolved over the past decade based on insights from direct customer feedback to Microsoft and to keep pace with the constantly changing threat landscape that customers face.

Still, some security industry observers and security researchers question why some Microsoft security updates sometimes take long periods of time to release. Opinions in the industry on the topic of “time to fix” vary, but the priority for security updates at Microsoft is to minimize disruption to customers and to help protect against online criminal attacks.

Microsoft uses a multipronged approach to help our customers manage their risks. This approach includes three key elements:

- **High-quality security updates** — Using world class engineering practices produces high-quality security updates that customers can confidently deploy to hundreds of millions of diverse systems in the computing ecosystem and that help customers minimize disruptions to their businesses.

- **Community-based defense** — Microsoft partners with many other parties when it investigates potential vulnerabilities in Microsoft software. Microsoft looks to mitigate exploitation of vulnerabilities through the collaborative strength of the industry and through partners, public organizations, customers, and security researchers. This approach helps to minimize potential disruptions to our customers’ businesses.

- **Comprehensive security response process** — Using a comprehensive security response process helps Microsoft effectively manages security incidents while providing the predictability and transparency that customers need to minimize disruptions to their businesses.

- For more information about this approach, see “Software Vulnerability

\(^4\) For more information on the Microsoft Security Response Center (MSRC), see [www.microsoft.com/msrc](http://www.microsoft.com/msrc)
Management at Microsoft™ at

Managing Security Updates by Using Microsoft Solutions

This section covers:

- Three approaches to managing security updates by using Microsoft products. Each of the following approaches has unique advantages and considerations:
  1. An update process that relies on Microsoft Update and Automatic Updates.
  2. An update process that relies on Windows Server® Update Services (WSUS).

At the end of this section, IT pros should:

- Understand the needs and considerations for using Microsoft Update and Automatic Updates to manage security updates:
  
  **Note:** IT pros and organizations that only require a managed security update process using Microsoft Update and Automatic Updates should only read this section.

- Understand the needs and considerations for using WSUS to manage security updates.
  
  **Note:** WSUS does not support deployment of non-Microsoft updates.

- Understand the needs and considerations for using Configuration Manager in Microsoft System Center to manage security updates.
  
  **Note:** Among many other features, Configuration Manager 2007 supports the deployment of Microsoft updates and non-Microsoft updates.

Microsoft resources referenced in this section:

- **Microsoft Update.** This is a free, built-in service that is included with Windows®. It provides a single location for getting updates and scheduling automatic updating. In addition, IT pros can get security and non-security updates for Microsoft software, such as the Microsoft Office system and Windows Live®. See update.microsoft.com/microsoftupdate.

- **Windows Server Update Services.** Use this to fully manage update settings

- **Microsoft System Center Configuration Manager 2007.** Use this with large, complex, and heterogeneous IT infrastructures to comprehensively assess, deploy, and update servers, clients, and devices across physical, virtual, distributed, and mobile environments. See microsoft.com/systemcenter/configurationmanager.

  - **Note:** To customize updating for compliance assessment, see technet.microsoft.com/library/bb633119.aspx.

### Three Approaches to Security Updates

Microsoft has developed a comprehensive suite of software update tools that can automatically update computers to help them stay protected against malicious software attacks. However, for various reasons, some individuals or organizations may consider other methods for updating their Microsoft software. With this in mind, Microsoft has developed various solutions to help IT pros who have varying needs to stay as up to date as possible within their own specific environments. There are many approaches to managing security updates, but this section outlines the following three approaches that use Microsoft software update solutions to address the security updating needs of Windows customers:

1. Use an update process that relies on Microsoft Update and Automatic Updates.
2. Use an update process that relies on Windows Server Update Services (WSUS).
3. Use an update process that relies on Microsoft System Center Configuration Manager 2007.

#### Update Process That Relies on Microsoft Update and Automatic Updates

<table>
<thead>
<tr>
<th>Intended Customer</th>
<th>Consumers and small businesses (typically, those with fewer than 50 computers).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need</td>
<td>To ensure that all systems are always up to date with the latest Microsoft security updates.</td>
</tr>
<tr>
<td>Advantages and Considerations</td>
<td>The security update can be installed with minimal or no user interaction and there is no need to understand the technical details of the security update. Ensure your organization does not have line-of-business (LOB) applications or other custom applications that could be affected by Microsoft security updates.</td>
</tr>
<tr>
<td>Price</td>
<td>Available for all IT pros at no cost.</td>
</tr>
</tbody>
</table>
Through the Automatic Updates feature, and when customers opt in through Microsoft Update, Windows can automatically keep the computer up to date with the latest security updates for all Microsoft products. Users do not have to search for updates and information; Windows delivers them directly to the computer. Windows recognizes when a system is online and uses the Internet connection to search for downloads from the Microsoft Update website.

Users can specify how and when Windows should update the computer. For example, users can set up Windows to automatically download and install updates on a schedule that the user specifies, as shown in Figure 6.

Figure 6. Automatic update settings in Windows 7

![Automatic Update Settings](image)

This approach is recommended for individual users or for users in small business environments who do not have a dedicated IT support function. Using this approach, computers can stay updated with minimal technical “know-how” and with a minimal number of interruptions to computer usage.
To verify current settings and to check for the latest updates, see update.microsoft.com/microsoftupdate.

### Update Process that Relies on Windows Server Update Services (WSUS)

<table>
<thead>
<tr>
<th>Intended Customer</th>
<th>Medium or large businesses (typically, those with more than 50 computers).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need</td>
<td>To fully manage update settings and control the distribution of updates for computers on customer networks.</td>
</tr>
<tr>
<td>Advantages and Considerations</td>
<td>WSUS does not support deployment of non-Microsoft updates.</td>
</tr>
<tr>
<td></td>
<td>Configurable options enable IT pros to collect inventory reports of managed devices, determine which updates apply to a computer or group of computers, specify the required update action, and then install updates based on a flexible schedule with little or no user intervention.</td>
</tr>
<tr>
<td></td>
<td>The process lessens the perceptible impact on employee productivity and network functionality.</td>
</tr>
<tr>
<td></td>
<td>Create custom reports such as security updates required by specific computers; provide notification and schedule automatic distribution of security updates.</td>
</tr>
<tr>
<td></td>
<td>Target specific nodes with a security update.</td>
</tr>
<tr>
<td></td>
<td>Manage multiple servers from a single console for more complex networks with server hierarchies.</td>
</tr>
<tr>
<td>Price</td>
<td>Available at no charge for licensed users of supported versions of Windows Server.</td>
</tr>
</tbody>
</table>

For organizations that have a dedicated IT support function, and want a higher degree of control over when and how security updates are distributed to the organization’s Windows clients and Windows servers, WSUS (see technet.microsoft.com/en-us/WSUS/default) is available at no charge for users who have a valid Windows Server license. WSUS enables administrators to control the
deployment of Microsoft security updates on Microsoft products that run a supported version of the Windows server or client products. Using WSUS, administrators can better manage the distribution of updates released through Microsoft Update to the computers on their network.

Some notable features of using a WSUS-managed security update approach include the following:

- WSUS only supports deployment of Microsoft updates.
- Specify updates by:
  - Product or product family (for example, Windows Server® 2008 or Microsoft Office).
  - Update classification (for example, critical updates and drivers).
  - Language (for example, English and Japanese only).
- Schedule for synchronization to initiate automatically, enforce a deadline, and set a specific date and time to install or uninstall updates. The administrator can force an immediate download by setting a deadline for a time in the past.
- Set up email notification for new updates and reporting functionality based on update status, computer status, computer compliance status, and update compliance status.
- Administrators can perform targeting tasks such as:
  - Deploying new updates to a test computer group, and then evaluating the updates before distributing them to the production environment.
  - Protecting computers that run specific applications. For example, if a critical update is incompatible with an application that certain computers use, an administrator can make sure that the update is not distributed to those computers.
- Achieve better performance and bandwidth optimization.

<table>
<thead>
<tr>
<th>Update Process that Relies on System Center Configuration Manager 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intended Customer</strong></td>
</tr>
<tr>
<td><strong>Need</strong></td>
</tr>
</tbody>
</table>
Update Process that Relies on System Center Configuration Manager 2007

<table>
<thead>
<tr>
<th>Advantages and Considerations</th>
<th>The process supports management and distribution of Microsoft and non-Microsoft software updates and applications.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The process ensures that the organization’s IT systems comply with desired configuration states to improve the availability, security, and performance of systems across the whole network.</td>
</tr>
<tr>
<td></td>
<td>The process provides advanced administrator control and awareness that WSUS does not include, such as delivering updates for Microsoft products; other applications; custom, in-house, LOB applications; hardware drivers, and so on.</td>
</tr>
<tr>
<td></td>
<td>Deploy system changes to servers and client computers at predetermined times and dates by using maintenance windows.</td>
</tr>
<tr>
<td></td>
<td>Better manage the user experience by displaying a customizable user interface and maintaining fine control over enforcement settings, such as restart and installation.</td>
</tr>
</tbody>
</table>

Price

See www.microsoft.com/systemcenter/configurationmanager/en/us/pricing-licensing.aspx or, if you are outside the United States, please contact your local Microsoft representative or partner.

For organizations that want to add another level of functionality and control to the security update process, this approach uses Configuration Manager 2007 to manage the WSUS environment and allows additional update control and deployment methods.

If WSUS is free, why pay for this approach? This solution provides several capabilities in the areas of advanced administrator control and awareness that WSUS does not include. In particular, IT pros can deliver updates for Microsoft products; other applications; custom, in-house, LOB applications; hardware drivers; and basic input/output systems (BIOS) to various devices including desktop computers, portable computers, servers, and mobile devices. IT pros can enable quarantine support by using Network Access Protection (NAP) and create collections based on inventory characteristics of computers. This enables administrators to better target their updates, while also performing functions such as:

- Managing Microsoft and non-Microsoft updates. Administrators can use one product for all management tasks, rather than a separate tool for update management.
- Deploying updates based on service windows (advertisements).
- Better managing the user experience by displaying a customizable user interface and maintaining fine control over enforcement settings such as
restart and installation.

- Fully understanding the compliance state of their environment through inventory information and detailed status about the system state of the computers they manage with respect to update deployments.

IT pros can also extend the capabilities of Configuration Manager 2007 through Desired Configuration Management (DCM), its native software development kit (SDK), and independent software vendor (ISV) partner contributions. Using DCM, IT pros can use Microsoft and other best-practice configuration knowledge to improve configuration definition and maintenance.

For more information about Configuration Manager 2007, see www.microsoft.com/systemcenter/configurationmanager/.

For more information about how to use Configuration Manager 2007 to provide these enhanced update features, see Configuring Software Updates at technet.microsoft.com/library/bb633119.aspx.

In the rest of this guide, the update process that relies on WSUS is discussed because this approach presents a solid baseline practice for a configurable and portable risk management framework for Microsoft security update releases.

**The Microsoft Security Update Release Process**

This section covers:

- The Microsoft process for testing and releasing security updates.
- Starting the Microsoft security update release process, which begins with a notification from Microsoft.
- The various Microsoft security release notifications and security updates:
  - The Microsoft Security Bulletin Advance Notification Service
  - Security bulletin summaries
  - Security bulletins
  - Security updates
  - Knowledge Base articles
  - Security advisories
- Fraudulent email messages that target security updates.
A customer risk-management framework to initiate upon receipt of a Microsoft security release that involves the following stages:

- Stage 1: Receive Microsoft Security Release Communications
- Stage 2: Evaluate Risk
- Stage 3: Evaluate Mitigation
- Stage 4: Use the Standard Deployment Timeline
- Stage 5: Monitor Systems
- Stage 6: Use Microsoft Resources to Track Security Developments

At the end of this section, IT pros should:

- Understand the guidance and various resources that accompany Microsoft security updates.
- Have a reference for a customer risk-management framework that can map Microsoft resources and guidance about security updates.
- Understand that Microsoft does not distribute security updates by email attachments. See support.microsoft.com/kb/959318 for more information on this.
- Microsoft encourages IT pros to obtain Microsoft security updates by using the links in this guide, the security bulletins, or deployment tools such as Microsoft Update, Windows Update, WSUS, or Configuration Manager 2007.

Microsoft resources referenced in this section:


How Microsoft Tests Security Updates

Microsoft security updates are delivered to hundreds of millions of computers around the world running many different combinations of operating system versions, language packs, device drivers, commercial software, and custom-
developed programs.

Updates that are not adequately tested before release could potentially cause problems for a large number of computers engaged in mission-critical activities. To minimize the chances of this happening, Microsoft subjects security updates to a rigorous testing process before releasing them to the public. The efforts outlined below have helped to significantly increase the quality of Microsoft security updates over the last five years. These quality improvements have enabled some customers to reduce the amount of testing they perform on Microsoft security updates, reducing the resources and costs associated with such work within their IT environments, and returning budget to fund other projects or reducing operating expenses to their corporations.

**Application Compatibility Testing**

Application compatibility is a fundamental underlying requirement for users of any operating system, productivity suite, or browser. Subtle changes in behavior can occur when an operating system is updated, potentially resulting in unpredictable behavior for applications. When mission critical and/or line-of-business applications fail to operate as expected, business is disrupted.

Therefore, application compatibility testing is a key component to the Microsoft approach to developing and releasing security updates for its products.

Minimizing application compatibility issues through security updates involves both depth and breadth testing. When a security update affects multiple versions of Windows or multiple versions of Windows Internet Explorer, for example, the test matrix grows rapidly as do the test plans required to ensure a very high level of confidence in the quality of the update. Security updates affecting Windows are tested on all supported versions of the operating system including Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. For enterprise customers who take advantage of the Microsoft Custom Support Program, Windows 2000 and/or Windows NT 4.0 might also be added to the test matrix (though this support option for Windows NT 4.0 ended in July 2010). Different SKUs of affected versions of Windows might also be tested (for example, Home Basic, Home Premium, Business, and Ultimate).

Different service packs for Windows and hotfixes (QFEs) are part of the test matrix for security updates. Affected versions of Windows are also tested in many different languages (Arabic, Chinese, German, Japanese, Russian, and others) as well. Because Windows is available for a wide variety of computing architectures, all of the testing is completed on the various architectures (that is, x86, x64, and Itanium). Thousands of the world's most used Windows applications are tested across these architectures, Windows versions, service pack levels, and languages.

This large test undertaking to address multiple architectures, products, and versions is a key way that Microsoft minimizes disruptions to enterprise customers.
Rootkit Detection

In February 2010, a number of computers experienced repeated “blue screen” stop errors after Microsoft Security Bulletin MS10-015 was installed. These problems were caused by the malware family Win32/Alureon, some variants of which include a rootkit component that makes unauthorized modifications to the kernel of an infected computer. These modifications conflicted with the kernel changes introduced by the initial version of the MS10-015 security update, causing the stop errors. The Microsoft Security Response Center (MSRC) subsequently addressed the issue with a revised version of the update.

To prevent problems like this from happening again, every security update that modifies the Windows kernel now includes a rootkit detection component that checks the state of the kernel before the update is installed to determine if the kernel has been tampered with by malware. If an irregularity is detected, installation stops and the installer displays a dialog box that directs the user to a Microsoft Knowledge Base article with information about the problem and how to resolve it.

Security Test Pass

Microsoft IT (MSIT) provides information technology services internally for Microsoft employees and resources. MSIT manages 900,000 devices for 180,000 users across more than 100 countries and regions worldwide. Computers managed by MSIT run many different combinations of operating system versions, language packs, device drivers, commercial software, and custom-developed programs. The breadth and diversity of this environment makes it an ideal test bed for verifying the stability and quality of security updates under realistic conditions, through a process called Security Test Pass.

Security Test Pass involves a group of about 24,000 computers used by Microsoft employees in various capacities. These computers are selected to reflect a diversity of user scenarios that cannot be provided in a controlled laboratory environment. Each update must be tested on a set minimum number of client computers and datacenter servers, and be installed alongside a minimum number of line-of-business applications. (In practice, this means deploying the test update to a much larger number of computers than the minimum, as not every computer will need the update being offered.)

The Security Test Pass process typically starts about three weeks before a security update is scheduled to be released, although this process can be expedited in the case of urgent “out-of-band” releases. The update is silently deployed to the test computers from a group of internal update servers. Deployments often fall into rounds, so that the most recent version of the update is being deployed at any given time. Each update is only subjected to Security Test Pass when development is complete and the product team believes that the update has reached a level of quality appropriate for release to the general public. Therefore, ideally testers should not experience any disruption from installing Security Test
Pass updates.

MSIT collects telemetry from Security Test Pass installations to discover any issues, conflicts, or interoperability problems that arise. In addition, testers are instructed to report any issues they encounter to MSIT, which has a dedicated support structure for Security Test Pass users. If a security update causes issues, the product group development team will work directly with the customer to determine the root cause and develop an immediate resolution. MSIT compiles a daily report of progress and issues and distributes it to Security Test Pass stakeholders.

**Security Update Validation Program**

To further minimize the potential for disruption, in 2005, Microsoft started the Security Update Validation Program (SUVP) (www.microsoft.com/technet/security/bulletin/info/suvp.mspx). The SUVP seeks to ensure the quality of security updates by testing them in environments, in configurations, and against applications, such as line-of-business (LOB) applications that Microsoft cannot easily duplicate. As a part of this quality control program, Microsoft makes security updates available to a limited group of customers, under a strict non-disclosure agreements (NDA), providing a way for customers to test updates in a broad range of configurations and environments before the updates are released for general availability. Participants are required to provide feedback based on their deployment experience to help identify potential compatibility problems before the MSRC releases the updates to the public. This program provides only the security updates to participants of the SUVP. Participants are not given any information about the underlying vulnerabilities, the area of code being updated, or information about how to exploit the vulnerabilities. The program has reduced compatibility issues and helps enhance the quality of security updates significantly, making it easier for customers to deploy updates more quickly. If you have questions about the SUVP program, you can send them to suvprog@microsoft.com.

**Microsoft Security Release Communications**

When there is material information about a vulnerability that threatens the security of its products, Microsoft sends out notifications and advisories to customers. These include:

**Security Bulletin Advance Notification**

A security bulletin advance notification contains information about the number of new security bulletins being released, the products affected, the aggregate maximum severity, and information about detection tools relevant to the update. The level of detail included is balanced against a need to protect organizations until the release of the security updates by not disclosing any information that could facilitate attacks. To help ensure against surprises and to minimize possible confusion, the security bulletin advance
notification also provides information about other updates that will be released on the same day that are not associated with security bulletins. Specifically, it details how many non-security updates will be released through Microsoft Update and Windows Update, in addition to any updates to the MSRT.

Where possible, Microsoft makes this notice available three business days before a security bulletin is released. This advance notification helps IT pros to plan the appropriate resources for the impending security update release. For more information, see the Microsoft Security Bulletin Advance Notification page at www.microsoft.com/technet/security/bulletin/advance.mspx.

Occasionally, some security bulletins are listed in the security bulletin advance notification but are not released when the security bulletin summary replaces the security bulletin advance notification. This is because Microsoft tests the quality of its security updates until they are released. If Microsoft locates a quality issue between the time when the security bulletin advance notification is released, and the time when Microsoft releases a security bulletin and its corresponding security update, Microsoft may delay the release of the security bulletin and security update. Sometimes, depending on the impact to an organization’s security update planning, Microsoft may rerelease its security bulletin advance notification to reflect this.

**Security Bulletin Summary**

When the security bulletins and security updates are released, the security bulletin advance notification is replaced by the security bulletin summary, which is the definitive resource for information about the security bulletins that the release includes. In addition to the information in the advance notification, security bulletin summaries contain an assessment of each vulnerability’s potential exploitability. (This is known as the “Exploitability Index,” and it is explained later.) For more information about Microsoft security bulletin summaries and webcasts, see www.microsoft.com/technet/security/bulletin/summary.mspx.

**Security Bulletin**

The security bulletin summary includes links to each security bulletin that the release includes, in addition to any related Knowledge Base articles that provide extra technical information to help IT pros with risk evaluation. Each security bulletin contains detailed guidance and information about the security update and the vulnerability. Security bulletins are localized in 19 languages, and contain frequently asked questions, vulnerability information, mitigations and workarounds, and other pertinent security update information. For more information, see the Microsoft Security Bulletin Search page at www.microsoft.com/technet/security/current.aspx.

**Security Update**

The security update is the download that contains the files that
address the security vulnerabilities that the security bulletin describes. These files are required to apply the update and can be tested and deployed to the required computers in the organization. There is information later in this guide about obtaining, testing, and deploying the security updates.

A single security update often addresses multiple vulnerabilities from the Common Vulnerabilities and Exposures (CVE) database; each of which is listed in a corresponding Microsoft security bulletin along with any other relevant issues. Whenever possible, the MSRC consolidates multiple vulnerabilities that affect a single binary or component and addresses them with a single security update. By doing so, the MSRC can maximize the effectiveness of each update, while minimizing the potential disruption that IT pros face from testing and integrating individual security updates into their computing environments.

**Knowledge Base (KB) Articles**

Microsoft Customer Service and Support (CSS) writes Knowledge Base (KB) articles that link to the corresponding security bulletin without duplicating all of the same information in the security bulletin. Knowledge Base articles are also released to highlight known caveats or issues with security updates and will continue to be referenced in the security bulletin that provides the security updates.

**Security Advisory**

Microsoft security advisories, localized in 19 languages, are communications from Microsoft about potential vulnerabilities and other security information that is material to an IT pro’s overall security. These notifications may not require a security bulletin or a security update, but may still affect customers’ overall security. Some security advisories may result in the release of a security update or may include guidance to help IT pros mitigate the threat that is posed. Each security advisory is accompanied by a unique Knowledge Base article number that references additional information. Some examples of topics that security advisories may discuss include:

- Guidance and mitigations that may be applicable for publicly disclosed vulnerabilities.
- Clarifying information about potential threats that are publicly disclosed.

**Predictable Security Update Release Process**

To make it possible to better predict security update releases and assist IT pros and organizations with resource planning, Microsoft has a standard security...
update release process. This process always starts with a security bulletin advance notification that informs IT pros of an impending security update release. When it is released, the security bulletin provides the technical details of the accompanying security update and the change that is required. Although security advisories are not as predictable, they are another form of Microsoft security release. Similar to the security bulletin advance notification, Microsoft notifies IT pros when security advisories are released. (There is information later about the notifications.) Regardless of whether the Microsoft security release is an advance notification of a security bulletin and the accompanying security update, or a security advisory, it is important for IT pros to take action and initiate a risk-management process upon receipt of the notification.

A Microsoft Security Release. For the purposes of this guide, “Microsoft security release” refers to a security notification from Microsoft that requires a customer to take action and manage the security risk. Again, this specific notification always starts with either a security bulletin advance notification or a security advisory and IT pros must initiate their own risk-management process. Typically, a host of other resources that Microsoft makes available are combined with any Microsoft security release. This guide details these resources as they apply to a customer risk-management framework.

Expansive Resources and Guidance. Microsoft security releases usually include a host of other supporting resources, guidance, tools, and so on. This guide examines the various Microsoft resources that are available throughout the risk-management process. Figure 7 details the Microsoft security releases and accompanying authoritative guidance and files. Information is included later in this guide about the various other resources that are available with Microsoft security releases.

Figure 7. Microsoft security releases and accompanying authoritative guidance and files

<table>
<thead>
<tr>
<th>Microsoft Security Release</th>
<th>Accompanying Guidance</th>
<th>Accompanying Files</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Knowledge Base Article(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Update(s)</td>
</tr>
</tbody>
</table>

*other resources and guidance are discussed later*
Fraudulent Notifications That Target Microsoft Security Updates

Email messages that claim to be security email messages from Microsoft and contain an attached executable file are never legitimate. Such email messages are bogus, or they are spoofs, and the attachments may contain malicious software. IT pros who receive email messages that claim to distribute a Microsoft security update are encouraged to delete the message and not open the attachment.

**Microsoft does not distribute Security Updates by using email attachments.** Email messages about security notifications from Microsoft always encourage IT pros to obtain Microsoft security updates by using the links in this document, the security bulletins, or deployment tools such as Microsoft Update, Windows Update, WSUS, or Configuration Manager 2007. (Additional information is included later in this guide about obtaining security updates.)

If an attachment is opened in one of these hoax email messages, Microsoft urges IT pros to run a full antivirus scan on the computer in which it was opened as soon as possible to help ensure no malicious software was installed. In addition, IT pros can run a free online computer safety scan. To do this, see safety.live.com.

For more information about recognizing and avoiding fraudulent email messages to Microsoft customers, see www.microsoft.com/protect/yourself/phishing/msemail.mspx.

Customer Risk Management Framework

To help illustrate guidance, resources, and tools that are available from Microsoft with every security release, this guide employs a general customer risk-management framework to serve as a backdrop. In this guide, the “customer risk management framework” refers to a general risk-management framework or timeline that IT pros can follow to understand and utilize the security release resources that Microsoft makes available. Figure 8 identifies the major stages of the customer risk-management framework (a more detailed version is available in the Appendix). The framework is best organized and presented as a timeline.

The risk-management framework in this guide incorporates five major stages.
Each stage details the various Microsoft resources and helpful tips so IT pros are better informed to manage risk. The five major stages of the risk framework used in this guide include:

1. Receiving the Microsoft security release communications
2. Evaluating the risk
3. Evaluating any mitigations or workarounds
4. Creating, testing and deploying the security update to either a standard or a more urgent timeline
5. Monitoring systems

Although the stages identified in Figure 8 appear straightforward, in practice, organizations have complex infrastructures that have varying levels of security risk and differing levels of management and support. For example, some organizations might follow a standard update timeline that can be shortened or expedited in the event of an urgent security update. This framework’s primary intent is to articulate where security resources and guidance from Microsoft fit throughout a risk-management framework to better inform IT pros in an all-inclusive reference document.

Relating to the above, it is important for IT pros to understand several key points:

1. **The security update process can be complex.** This is especially true in organizations that support many business applications and custom line-of-business (LOB) applications. However, there are several solutions that make a successful security update process achievable.

2. **Understanding security update approaches is vital.** IT pros should select the most suitable approach that is required to support all of the applications in the organization (including third-party updates and LOB applications).

3. **IT pros need to balance the cost of implementation against the business risk.** This is a difficult process. The intention of this guide is to help IT pros understand the tools, services, and information that Microsoft makes available to help support this risk-management process.

4. **You must customize any framework and process to fit your organization.** The requirements for each organization are different, so plan for these requirements and customize them appropriately.

As this guide further examines the stages in the Microsoft security release
framework, IT pros should see how they can use the information that Microsoft provides to make the best decisions for their organizations.

If your organization does not have any risk-management approach in place, the section “Stage 2: Evaluate Risk” in this guide provides some options.

Stage 1: Receive Microsoft Security Release Communications

This section covers:

- How IT pros can ensure that they receive all relevant Microsoft security notifications.

At the end of this section, IT pros should:

- Receive all Microsoft security release notifications.

Microsoft resources referenced in this section:

- MSRC blog. See blogs.technet.com/msrc/.

Microsoft Security Release Communications

Microsoft sends out a notification if there is material information that affects customers' security. If security changes are required, Microsoft releases a security update, which includes all of its supporting collateral such as the security bulletin, Knowledge Base article, and so on. Otherwise, Microsoft communicates
via several methods (for example, a security advisory or a blog post) on the matter that affects customers’ security and provides guidance along the way.

Microsoft schedules the release of the security update and the security bulletin on the second Tuesday of the month at 10:00 AM in the Pacific Time zone. (The security bulletin advance notification occurs three business days before this.) Depending on the time zone, or time zones, in which the organization operates, IT pros should plan their deployment schedules accordingly. If a security issue is so severe that Windows-based computers are at serious risk, and Microsoft has determined that a security change is immediately required out of the normal monthly cycle, Microsoft will issue an out-of-band security release.

Whether the security release is a security advisory, part of the standard monthly security update release, or an out-of-band release, Microsoft uses specific notifications. After an organization’s security team has received the Microsoft security notifications, it can better determine what security issues and updates may be relevant to the organization and plan for the steps that the organization needs to take.

**Receiving Microsoft Security Release Communications**

To help ensure that IT pros receive Microsoft security communications or notifications in a timely manner, Microsoft recommends that the appropriate IT support staff sign up for, at a minimum, the alerts that are identified in Figure 9.

Figure 9. Security alert signup

<table>
<thead>
<tr>
<th>Notification</th>
<th>Details</th>
</tr>
</thead>
</table>

* Depending on the time of year, this is Coordinated Universal Time (UTC) -8 or UTC -7.
### Comprehensive Security Alerts

The free comprehensive alerts provide advance notification of upcoming security bulletins (and thereby security updates), security advisories, and timely notification of any changes to Microsoft security bulletins or security advisories that were previously released. These notifications are written for IT pros, contain in-depth technical information, and the email messages are digitally signed with Pretty Good Privacy (PGP):

- **Email:** Security Notification Service Comprehensive Edition
- **RSS:** Comprehensive Alerts

You can access the aforementioned resources from [technet.microsoft.com/security/dd252948.aspx](http://technet.microsoft.com/security/dd252948.aspx).

### Microsoft Security Response Center (MSRC) blog alerts

The MSRC blog provides a real-time way for the MSRC to communicate with IT pros. The MSRC uses this blog to disseminate important and material security communications to help IT pros understand Microsoft security response efforts; updates during the early stages of security incidents; and regular postings for the bulletin release cycle:

- **RSS:** MSRC Blog
- **Windows Live Alert:** MSRC Blog
- **Website:** blogs.technet.com/msrc

### MSRC Twitter feed

The MSRC uses a verified Twitter account at [twitter.com/msftsecresponse](https://twitter.com/msftsecresponse) to post brief notifications about security bulletins, security advisories and other security issues. Follow @msftsecresponse via the Web, RSS, or SMS text message for fast access to the latest information.

### Trustworthy Computing Security and Privacy Blogs

This page dynamically consolidates and features blogs from the Microsoft Trustworthy Computing (TwC) Group: the team charged with working to deliver more secure, private and reliable computing experiences. Read about the long-term Microsoft vision and strategy for computing privacy and security.


When Microsoft makes available a new security release, it is vital that IT pros can rapidly determine the risk that their organization faces from the security issues or vulnerabilities that the release communicates. This guide provides details about some processes and decisions that IT pros need to make as applied to the
customer risk-management framework.

The stages in this guide focus on Microsoft security updates and advisories only. It may be possible for organizations to incorporate some recommendations into maintenance update processes for other update types such as service packs, driver updates, and others.

Stage 2: Evaluate Risk

This section covers:

- Applying Microsoft resources to a customer risk-management framework that determines:
  - Whether the vulnerability referenced in the security release applies to the organization.
  - What the risk, if any, the vulnerability referenced in the security release poses to the organization.
  - The resources Microsoft makes available to determine the vulnerability application and risk.
  - An example of a risk assessment that uses Microsoft resources.
  - Additional considerations before security update deployment.

At the end of this section, IT pros should:

- Understand key Microsoft resources to help determine the applicability of the vulnerability to their organization. Microsoft resources used to gather intelligence include:
  - The Microsoft product support life cycle.

- Understand key Microsoft resources to help determine the risk level within the organization. These include:
  - Security bulletins and security advisories.
  - Security bulletins and the Microsoft severity ratings system, and other vulnerability impact information.
  - The Exploitability Index, which discloses vulnerability risk if the security update is not applied.

- Understand other important considerations that are relevant at this point of
an organization’s risk-management framework, such as:

- Reviewing Knowledge Base articles.
- Assessing the ease of uninstalling a security update and whether a forced restart is required.

**Microsoft resources referenced in this section:**

- **Microsoft Security Risk Management Guide**. A technology-agnostic solution that provides a four-phased approach to risk-management. The guide references many industry accepted standards for managing security risk, and incorporates real-world experiences from Microsoft IT and also includes input from Microsoft customers and partners. See technet.microsoft.com/library/cc163143.aspx.

- **Microsoft Security Bulletin Search page.** This page is the central portal that is related to security bulletins. It provides information such as the latest Microsoft security bulletins and advisories, previous security bulletins, a capability to search for security bulletins and Knowledge Base articles, and more. See www.microsoft.com/technet/security/current.aspx.

- **Microsoft Product Lifecycle Search page.** Microsoft provides support on the current service pack, and in some cases the immediately preceding service pack, for products that you can reference from this page. See support.microsoft.com/lifecycle/search/.

- **MSRC blog.** The official corporate security response blog published by the Microsoft Security Response Center. See blogs.technet.com/msrc/.

- **Microsoft Security Research & Defense blog.** Information from Microsoft about vulnerabilities, mitigations and workarounds, active attacks, security research, tools, and guidance. See blogs.technet.com/srd/.

- **Microsoft Exploitability Index.** This Index helps IT pros to prioritize deployment of security updates. The Exploitability Index provides details about how exploitable a vulnerability may be, and the likelihood of exploit code being published in the month following a security bulletin’s release. (see technet.microsoft.com/security/cc998259.aspx). The Exploitability Index is contained in each security bulletin summary and webcast. See www.microsoft.com/technet/security/bulletin/summary.mspx.

- **Knowledge Base articles.** Search these at www.microsoft.com/technet/security/current.aspx or support.microsoft.com/.

---

Determinations in the Risk Management Framework

Without doubt, one of the most serious decisions that IT pros make in their risk-management framework is what risk a newly identified vulnerability poses to the organization. The deployment of a security update has an inherent cost both in terms of the test and deployment costs and the support costs of any issues that may result. The decision that IT pros need to make is whether this cost outweighs the risk the organization faces from a potential attack stemming from an “unpatched” system. Figure 10 details the inputs and the subsequent decisions appropriate for the Evaluate Risk stage.

Figure 10. Evaluate Risk stage
Determinations in this stage. As Figure 10 illustrates, IT pros need to identify two things at this stage:

1. Does the vulnerability apply to the organization? Or asked another way, does the vulnerability referenced in the Microsoft security release apply to the organization?

2. Does the vulnerability represent a risk high to the organization? Or asked another way, what does the risk that the vulnerability addressed in the Microsoft security release pose to the organization?

The remaining sections for this stage of the guide includes details on important considerations to help IT pros produce informed answers to these questions that are appropriate before deploying security updates.

Identify Whether the Vulnerability Applies

After the Microsoft security release notification is received, the first determination to make during the Evaluate Risk stage of a customer risk-management framework is whether the vulnerability in question applies to the organization. To make an informed decision, this section explores Microsoft resources for gathering the necessary security intelligence to make a more informed decision.
Gathering Security Vulnerability Intelligence

IT pros need to gather and evaluate several vital pieces of information to determine exactly how much risk the organization can be exposed to before a security control or security update is in place. Microsoft uses some important communication to ensure that organizations understand the risk that a vulnerability poses to the IT infrastructure and the organization’s overall security. Figure 11 highlights Microsoft resources that we recommend using in order to gather the necessary security intelligence to properly identify whether the vulnerability applies to your organization.

Figure 11. Microsoft security release information sources

<table>
<thead>
<tr>
<th>Determination</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify if the product is affected.</td>
<td>Microsoft notifies IT pros of products that are affected by vulnerabilities in the following ways:</td>
</tr>
<tr>
<td></td>
<td>Security bulletin summaries inform IT pros of the affected product or software family in the “Executive Summary” section. For example, if Windows is listed under the “Affected Software” section, this could mean that any of the currently supported Windows operating systems are affected.</td>
</tr>
<tr>
<td></td>
<td>Security bulletin summaries enable IT pros to quickly assess whether a security bulletin, and thereby a security update, applies to their organization. Another example, if IT pros do not use Windows® Internet Explorer® and they review a security bulletin summary that lists Internet Explorer as affected software, they can simply dismiss the related security bulletin and security update.</td>
</tr>
<tr>
<td></td>
<td>Security bulletins and security advisories identify the affected product or software more specifically than the security bulletin summary (using the above Windows example, among other versions of Windows®, Windows® XP Service Pack 3 (SP3) might be listed under “Affected Software”).</td>
</tr>
<tr>
<td></td>
<td>Sources to check affected products:</td>
</tr>
<tr>
<td></td>
<td>✦ To review security bulletins, see <a href="http://www.microsoft.com/technet/security/current.aspx">www.microsoft.com/technet/security/current.aspx</a>.</td>
</tr>
<tr>
<td></td>
<td>✦ To review security advisories, see <a href="http://www.microsoft.com/technet/security/advisory">www.microsoft.com/technet/security/advisory</a>.</td>
</tr>
<tr>
<td></td>
<td>Some other organizations also offer their own analyses of</td>
</tr>
<tr>
<td>Determination</td>
<td>Details</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>Microsoft security updates. These analyses should be treated with caution, as Microsoft is the definitive expert on its own updates.</td>
</tr>
<tr>
<td></td>
<td>Finding the affected products and components. In the security bulletin or the security advisory, see the “Affected Software” section for more specific affected product information.</td>
</tr>
<tr>
<td></td>
<td>Each security bulletin further details the affected software by including both affected and non-affected software (for example, affected operating systems: Windows® XP SP3; non-affected software: Windows Vista® SP1).</td>
</tr>
<tr>
<td></td>
<td>Security advisories detail the affected and non-affected software in the “Overview” section, as the following sample security advisory illustrates.</td>
</tr>
<tr>
<td></td>
<td>Another helpful source in the security bulletin that identifies mitigating factors is the “Vulnerability Information” section. Go to the “Vulnerability Information” section, then expand the CVE identifier addressed by the security bulletin, and then finally expand “Mitigating Factors” to access additional information.</td>
</tr>
<tr>
<td></td>
<td>If the product is not listed in the “Affected Software” section or the “Overview” section, the vulnerability does not apply and the security update or additional countermeasure is not needed.</td>
</tr>
<tr>
<td>Determination</td>
<td>Details</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Review the Microsoft support life cycle of your applications and operating systems. | Organizations may be running versions of software that Microsoft no longer supports. As part of an organization’s risk-management process, IT pros should understand whether products in the IT environment are no longer supported because these products may have vulnerabilities that need to be mitigated to reduce the organization’s risk. It should be a priority for organizations that have older releases of the software to migrate to supported releases to prevent potential exposure to vulnerabilities. For more information about the security update support period for these software versions or editions, see support.microsoft.com/lifecycle/search/ and verify that Microsoft still supports the product. The affected software that is listed in Microsoft security bulletins has been tested with the security update to help ensure compatibility. However, older software releases that are past their support life cycle will not have been tested. For additional information, see the Windows Operating System Product Support Lifecycle FAQ at support.microsoft.com/gp/LifeWinFAQ. If custom support for older Microsoft product releases is required, contact the local Microsoft office. Alternatively, if the organization is an Alliance, Premier, or Authorized Contract holder, contact the respective Microsoft account team representative, the Technical Account Manager, or the appropriate Microsoft partner representative for custom support options. To find the local Microsoft office:  
2. In the Contact Information list, click the closest office to your primary business location, and then click Go. The website, office addresses and telephone numbers will be displayed.  
3. When calling, ask to speak with the local Premier Support sales manager. |
After IT pros have gathered and reviewed this information, they should be able to determine whether the security vulnerability applies to the organization.

**Determining the Vulnerability Risk**

After IT pros have confirmed whether the vulnerability applies to the organization, as shown in the diagram below, the next step in the Evaluate Risk Stage should be to identify what risk the vulnerabilities poses to the organization.

When a Microsoft security notification contains information about more than one security issue, IT pros must check each issue individually for its potential risk to the organization.

What is a High Risk? Invariably, vulnerability risks differ by organizations; and organizations typically have different thresholds for what is considered “high” risk and “low” risk – and many other risk ratings in between. As previously mentioned, the *Microsoft Security Risk Management Guide* can help IT pros
determine what appropriate risk levels are within an organization. For the purposes of this guide, the customer risk-management framework uses two risk levels – high and low. How your organization classifies this depends on a number of inputs, of which many are described below. The important point is that IT pros should first focus on mitigating the most severe vulnerabilities, which this guide defines as high risk.

The Microsoft Severity Rating System

One of the first inputs factored into the risk evaluation stems from the severity rating of the vulnerability. Microsoft conveys the vulnerability severity using the Microsoft severity rating system (see www.microsoft.com/technet/security/bulletin/rating.mspx).

The Microsoft Severity Rating System Explained. Microsoft is aware of several varying severity rating systems. For example, version 2 of the Common Vulnerability Scoring System (CVSS)\(^8\) rates vulnerabilities across all industry products. Assessing severity is a complex process that can vary by customer segment. Therefore, it is difficult for a single rating to represent the true risk of a vulnerability for all customers in all scenarios. As a result, an effective vulnerability rating system should be one that neither underrates nor overrates vulnerabilities. The goal is to best help the majority of customers accurately measure risk, and better inform customers to better enable them to make their own informed risk assessments.

Microsoft believes the primary source of vulnerability severity information should germinate from customer need and then be supplied by the product vendor; especially since vendors know their products best and can give the most informed guidance. Microsoft provides customers with authoritative guidance such as mitigations, workarounds, and descriptions of possible attack vectors to help customers perform their own risk analysis and management. Customers have informed the Microsoft Security Response Center that the severity rating system is valuable in helping them assess their level of risk. Customers also tell Microsoft that Microsoft security bulletins, advisories and the Microsoft severity rating system are all valuable in helping them assess their level of risk. Microsoft cautions on the side of worst-case-scenario when rating vulnerabilities as having a “maximum severity” of Critical, Important, Moderate or Low. And when dealing with a borderline rating situation, our experience has also shown that it is prudent to exercise caution on the side of the “worst-case” scenario.

What the severity ratings mean. Simply, the Microsoft severity ratings translate to the maximum potential impact of the attack. Microsoft evaluates each issue and quantifies an issue's impact objectively on a technical level for default

---

\(^8\) Microsoft is an active member of the CVSS-SIG and participates in discussions related to the current version of CVSS.
configurations. Based on this analysis and the maximum security impact, Microsoft supplies a rating in the security bulletin. Figure 12 defines the four Microsoft severity ratings and their corresponding impact.

Figure 12. Microsoft severity rating system

<table>
<thead>
<tr>
<th>Rating</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>A vulnerability whose exploitation could enable the propagation of an Internet worm with little or no user action.</td>
</tr>
<tr>
<td>Important</td>
<td>A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users’ data, or of the integrity or availability of processing resources.</td>
</tr>
<tr>
<td>Moderate</td>
<td>A vulnerability whose exploitation is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.</td>
</tr>
<tr>
<td>Low</td>
<td>A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.</td>
</tr>
</tbody>
</table>

For additional information about these criteria, see [www.microsoft.com/technet/security/bulletin/rating.mspx](http://www.microsoft.com/technet/security/bulletin/rating.mspx).

**Maximum and aggregate severity ratings.** It is worth noting that a security bulletin summary lists the maximum security rating for the affected product family while the security bulletins provide the further detail. For example, suppose that Windows is listed as affected software, Windows XP SP3 is listed as Critical, and Windows Vista is listed as Important. The security bulletin summary will state that the maximum severity rating for the respective bulletin is Critical; again applying the maximum severity rating for Windows. The security bulletin further details the maximum security impact and aggregate severity rating for each supported version of the affected software. See Figure 13 and Figure 14 for examples.

As shown in Figure 13 below, the “General Information” section of each Microsoft security bulletin contains a table that lists each product and component that the bulletin addresses, the maximum security impact, the aggregate severity rating, and the security bulletins that the update replaces.
Figure 13. Aggregated severity ratings in a Microsoft security bulletin

The severity ratings, along with the other resources listed in Figure 15 (see below), help give IT pros material information that can be used to better manage risk. Since some IT pros may require more in-depth technical details about the vulnerability that a security update addresses, each security bulletin contains more information about the vulnerability in a section titled “Vulnerability Information,” as Figure 14 illustrates. Among other details, this section details the vulnerability (as identified by its CVE identifier), the individual vulnerability severity ratings, and the maximum security impact on affected software.

Figure 14. Vulnerability information in a Microsoft security bulletin

Risks vary by organization. Before moving to the next stage in the risk-management framework, it is important to document the risk in a manner that clearly identifies the risk as it relates to your organization. The following section provides sources and information that IT pros can use to generate a risk rating that is customized to identify the risk as it applies to your organization.

Risk Evaluation Resources

Microsoft Exploitability Index: Through various communication channels, Microsoft has always provided customers with information about the availability of proof-of-concept (PoC) exploit code or active attacks related to vulnerabilities
addressed by Microsoft security updates. The Microsoft Exploitability Index was developed in response to customer requests for additional information to better evaluate risk; it provides new data on the likelihood of functioning exploit code being developed so customers have additional guidance to better prioritize the deployment of Microsoft security updates.

The information that Microsoft provides is designed to help customers understand the real-world risks (and real possibility) of published functioning exploit code being developed for vulnerabilities that are addressed by Microsoft security updates. This information enables customers to better identify the security updates that are most important to them and deploy them in a timely manner. The Exploitability Index has been included in all Microsoft security bulletins since October 2008, and it uses a three-level scoring system to rate the likelihood of functioning exploit code being developed for each vulnerability published in security bulletins.

A key metric for evaluating the Exploitability Index is the reliability of the index as a predictor of the potential risk of functioning exploit code being developed; also, when predictions prove later to be inaccurate, whether they “fail safely” and do not cause customers to inappropriately under-prioritize a security update. By sharing published exploitability ratings for Microsoft vulnerabilities, together with the identification of Microsoft vulnerabilities with public exploit code, customers gain valuable information about likely risks and the current levels of threat to Microsoft software.

Reliability is Important: No exploitability index can be 100 percent accurate, but Microsoft is committed to continuous engagement with customers, partners, and the security community to improve, validate, and verify the accuracy of the Exploitability Index. Although predicting activity within the security ecosystem is risky, this index is likely to have a high degree of reliability for the following reasons:

1. **Common methodology.** The methodology used by Microsoft to provide Exploitability Index information for an update is similar to that used by many security researchers to create and evaluate protections, and to create exploit code to test these protections. This methodology involves researchers analyzing Microsoft security bulletins when they are released in the same way that Microsoft developers analyze the bulletins to determine the nature of the vulnerability and the conditions that must be met for an exploit to execute successfully.

2. **Vulnerability analysis.** Microsoft carefully analyzes every vulnerability resolved by a Microsoft security update, which has provided valuable insights into the difficulty of creating exploit code that will work consistently. For example, not all vulnerabilities result in released exploit code; the Microsoft Security Intelligence Report (SIR)12 has shown in the past that approximately 30 percent of vulnerabilities that were resolved in Microsoft security bulletins resulted in the release of functioning exploit code. Although there are many social factors that can determine the release of
exploit code, the technical differences in vulnerabilities make exploitation even more challenging. For example, the combination of ASLR13 and DEP14 on Windows Vista® and Windows 7 makes some vulnerabilities more difficult to exploit. Other vulnerabilities require systems with memory in a predictable state for successful exploit code to function.

3. **Partner validations.** Microsoft is partnering with security software providers through MAPP to help validate predictions each month—Microsoft believes this kind of community approach and information sharing will ensure better accuracy.

Figure 15 identifies steps and Microsoft resources that an IT pro should consider as part of a risk-management framework to help determine the risk level for the organization.

**Figure 15. Risk evaluation steps**

<table>
<thead>
<tr>
<th>Risk evaluation steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine whether the affected software listed in the Microsoft security release is identified as “at risk” and exhibits the vulnerability that the update is designed to address.</td>
<td>Not all vulnerabilities pose the same risk to all IT environments; some vulnerabilities depend on configuration and usage scenarios. This step requires IT pros to determine whether the instances of the product or service in the organization are likely to exhibit the vulnerability as it is implemented. For example, a security update might be designed for all Windows Server operating systems running Internet Information Services (IIS) with Active Server Pages (ASP) enabled. Although an organization might contain several Windows Server operating systems, the security update is unlikely to be relevant if the organization does not have ASP enabled on any IIS servers. IT pros should check the “Affected Software” and “Non-Affected Software” sections in the security bulletin. Then read the CVE identifier entry in the “Vulnerability Information” section of the security bulletin, which includes mitigating factors that could reduce the severity of exploitation of a vulnerability and the associated content.</td>
</tr>
</tbody>
</table>
## Risk evaluation steps

<table>
<thead>
<tr>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Microsoft security blogs for additional technical information about security bulletins as applicable.</td>
</tr>
</tbody>
</table>

- The Microsoft Security Research & Defense blog ([blogs.technet.com/srd](blogs.technet.com/srd)) contains information about specific security bulletins, security updates, and security advisories. This can include additional technical information about vulnerabilities or active attacks, additional mitigations and workarounds, and other notes to aid in an IT pro’s risk assessment, which are not included in security bulletins or advisories.

  The bloggers on the Security Research & Defense blog are individuals from Microsoft who perform in-depth technical analysis of vulnerability reports; investigate and perform research on new vulnerabilities; provide technical guidance for security bulletins; and ensure that security updates are effective in eliminating software vulnerabilities.

- The MSRC blog ([blogs.technet.com/msrc](blogs.technet.com/msrc)) provides a roundup of new security bulletins and advisories as they are released, with additional insights from Microsoft security response engineers in the form of webcasts, in-depth analysis of individual vulnerabilities, and pointers to additional information. The MSRC also posts quick notifications about new blog entries and other late-breaking information on the Twitter messaging service at twitter.com/msftsecresponse.

- The Microsoft Malware Protection Center (MMPC) blog ([blogs.technet.com/mmpc](blogs.technet.com/mmpc)) provides a real-time method for the MMPC to communicate with customers. Topics include day-to-day, “behind the scenes” information about new, emerging and interesting malware threats as well as other research topics in the computer security field.
<table>
<thead>
<tr>
<th>Risk evaluation steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attend or view the interactive TechNet security bulletin webcast.</td>
<td>Register for upcoming, or view previous, TechNet security bulletin webcasts at <a href="http://www.microsoft.com/technet/security/bulletin/summary.mspx">www.microsoft.com/technet/security/bulletin/summary.mspx</a>. With every security bulletin release, Microsoft hosts a one-hour security bulletin webcast that routinely starts 25 hours after the release of the security updates. The session, hosted by Microsoft security subject matter experts, starts with a brief technical overview of the latest security bulletins. Much of the time is spent addressing customer questions or concerns in an interactive, question-and-answer online forum. For IT pros who cannot attend these webcasts live or want to review material afterward, after the webcast Microsoft regularly posts the security bulletin webcast question-and-answer script on the MSRC blog at <a href="http://blogs.technet.com/msrc/archive/tags/Security+Update+Webcast+Q_2600_3B00_A/default.aspx">blogs.technet.com/msrc/archive/tags/Security+Update+Webcast+Q_2600_3B00_A/default.aspx</a>.</td>
</tr>
</tbody>
</table>
Before applying the update to systems, determine what the cost is to the organization if the vulnerability is exploited.

It is important to understand that there is a risk associated with not applying a security update. If an identified vulnerability leads to a security breach or system instability before IT pros install the security update (as part of the standard update process), they must understand what the potential impact would be on the business. IT pros should prioritize change requests based on the potential impact of an attack on an “unpatched” system.

Check the “Vulnerability Information” section of the security bulletin, which details the maximum security impact of the vulnerability.

<table>
<thead>
<tr>
<th>Risk evaluation steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before applying the update to systems, determine what the cost is to the organization if the vulnerability is exploited.</td>
<td>It is important to understand that there is a risk associated with not applying a security update. If an identified vulnerability leads to a security breach or system instability before IT pros install the security update (as part of the standard update process), they must understand what the potential impact would be on the business. IT pros should prioritize change requests based on the potential impact of an attack on an “unpatched” system.</td>
</tr>
</tbody>
</table>

Check the “Vulnerability Information” section of the security bulletin, which details the maximum security impact of the vulnerability.

Microsoft Security Bulletin MS10-073 - Important
Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)
Published: October 12, 2010
Version: 1.0

General Information

Executive Summary
This security update resolves several publicly disclosed vulnerabilities in the Windows kernel-mode drivers. The most severe of these vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system or coerces normal users to log on to an affected system. These vulnerabilities could allow an attacker to control an affected system.

Vulnerability Information

Severity Ratings and Vulnerability Identifiers
The following severity ratings assume the potential maximum impact of the vulnerability. For information regarding the likelihood, within 30 days of the security bulletin release, of the exploitability of the vulnerability in relation to its severity rating and security impact, please see the Exploitability Index in the Security Bulletin Summary. For more information, see Microsoft Exploitability Index.

Vulnerability Severity Rating and Maximum Security Impact by Affected Software

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity Rating</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
<td>Important</td>
</tr>
<tr>
<td>Maximum Security Impact</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
<td>Important Elevation of Privilege</td>
</tr>
</tbody>
</table>

Then, under the “Vulnerability Information” section, read the Frequently Asked Questions (FAQs) for the respective vulnerability that is detailed in the bulletin. Typically, the MSRC addresses the maximum security impact with its first FAQ: “What is the scope of this vulnerability?”
### Risk evaluation steps

<table>
<thead>
<tr>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consider the likelihood of functioning exploit code being developed for the vulnerability.</td>
</tr>
<tr>
<td>Exploit code is a software program or sample code that, when it is executed against a vulnerable system, uses the vulnerability to spoof attacker identity, tamper with user or system information, repudiate attacker action, disclose user or system information, deny service to valid users, or elevate privileges for the attacker.</td>
</tr>
<tr>
<td>Functioning exploit code can cause the maximum security impact of a vulnerability to occur. For example, if a vulnerability had a security impact of remote code execution, functioning exploit code would be able to cause remote code execution to occur when it was run against a target system.</td>
</tr>
<tr>
<td>The Microsoft Exploitability Index provides additional information to help IT pros better prioritize the deployment of Microsoft security updates. This Index provides IT pros with guidance on the likelihood of functioning exploit code being developed for vulnerabilities addressed by Microsoft each security update within the first 30 days of its release.</td>
</tr>
<tr>
<td>Vulnerabilities for which there is a higher likelihood of functioning exploit code being developed should take deployment preference. In the “Key Notes” section, Microsoft details whether the vulnerability in the security bulletin is currently being exploited on the Internet.</td>
</tr>
<tr>
<td>The Exploitability Index is located in the security bulletin summary under the “Exploitability Index” section.</td>
</tr>
<tr>
<td>For more information about the Exploitability Index, see technet.microsoft.com/security/cc998259.aspx.</td>
</tr>
</tbody>
</table>
In some critical situations, when customers are believed to be at serious risk and a high-quality update can be developed and released quickly, Microsoft issues an out-of-band security update (that is, a security update release that does not adhere to the standard Microsoft security update release cycle).

Out-of-band security updates are unusual and not scheduled, so they must be given extra consideration and attention as a potential high risk.

To ensure that IT pros receive notifications about out-of-band Microsoft security updates, see the earlier section, “Stage 1: Receive Microsoft Security Releases.” In addition, if IT pros are unsure whether a Microsoft security update is out-of-band or delivered regularly through the monthly security update process, they can check the MSRC blog for real-time information at blogs.technet.com/msrc/.

This pertains primarily to security advisories because they often do not contain binaries that force a security change on a product. As a result, when IT pros receive a Microsoft security advisory, Microsoft urges them to review the “Suggested Actions” section and take action as appropriate.

Combining all of the security intelligence from the above table helps IT pros put together a snapshot of the risk that the vulnerability presents, which might look like something like the below.

<table>
<thead>
<tr>
<th>CVE Identifier</th>
<th>Microsoft severity rating</th>
<th>Exploitability Index assessment</th>
<th>Comment</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-20YY-XXXX</td>
<td>Critical</td>
<td>1</td>
<td>Consistent exploit code is likely. Potential Remote Code Execution (RCE).</td>
<td>Current exploits in the wild</td>
</tr>
<tr>
<td>CVE-20YY-XXXX</td>
<td>Critical</td>
<td>1</td>
<td>Consistent exploit code is likely. Potential RCE.</td>
<td>Responsibly Disclosed</td>
</tr>
<tr>
<td>CVE Identifier</td>
<td>Microsoft severity rating</td>
<td>Exploitability index assessment</td>
<td>Comment</td>
<td>Note</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------</td>
<td>---------------------------------</td>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>CVE-20YY-XXXX</td>
<td>Critical</td>
<td>1</td>
<td>Consistent exploit code is likely. Potential RCE.</td>
<td>Responsibly Disclosed</td>
</tr>
</tbody>
</table>

**Affected Products**
Windows XP SP3, Windows Server 2003 SP2

**Affected Components**
DirectX® 7, DirectX 8.1, DirectX 9.0/9.0a/9.0b/9.0c

**Possible Attack Vectors**
Open a specially crafted QuickTime file or receive a specially crafted streaming content from a website or any application that delivers web content.
Content could be sent through email or hosted on a website.
Content hosted on a network share. Simply hovering the mouse over the file could cause a crash.

**Impact of Attack**
The attacker could gain the same rights as the logged on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**Mitigating Factors**
An attacker would have no way to force users to visit a specially crafted website or open a specially crafted file.
All supported versions of Windows Vista, Windows 7, and Windows Server® 2008 are not affected.

**Additional Information**
This security update addresses the issue in Microsoft Security Advisory XXXXXX.

**Other approaches?** Of course there are many approaches to evaluate the risk presented by a security vulnerability. As an example, some organizations feel the aforementioned level of analysis required to determine the vulnerability risk is laborious and counterproductive. Such organizations might therefore feel it is of greater value to skip those steps altogether and treat all security updates as equal. They can simply move into the next stage or right into the creation, testing, and deployment of the security update package.

**Example: Applying Microsoft Guidance to Evaluate Risk**

The following section applies solely to Microsoft security updates (that is, not to Microsoft security advisories, which do not contain this information). The following steps can help IT pros determine factors that could affect the risk that the organization could face before they implement a countermeasure or security update. For this example, suppose that, in one month, the MSRC releases five
new security bulletins that have the severity ratings that Figure 17 describes.

Figure 17. Example of the Severity Rating System

<table>
<thead>
<tr>
<th>Security Bulletin</th>
<th>Vulnerability identifier</th>
<th>Microsoft severity rating</th>
<th>Risk rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSYY-001</td>
<td>CVE-20YY-AAAA</td>
<td>Critical</td>
<td>...</td>
</tr>
<tr>
<td>MSYY-002</td>
<td>CVE-20YY-BBBB</td>
<td>Critical</td>
<td>...</td>
</tr>
<tr>
<td>MSYY-003</td>
<td>CVE-20YY-CCCC</td>
<td>Important</td>
<td>...</td>
</tr>
<tr>
<td>MSYY-004</td>
<td>CVE-20YY-DDDD</td>
<td>Moderate</td>
<td>...</td>
</tr>
<tr>
<td>MSYY-005</td>
<td>CVE-20YY-EEEE</td>
<td>Critical</td>
<td>...</td>
</tr>
</tbody>
</table>

The Microsoft bulletin severity ratings assume the worst-case attack scenario. Based on this information, IT pros might decide to expedite the MSYY-001, MSYY-002, and MSYY-005, and to use the standard update timeline to deploy MSYY-003 and MSYY-004.

**Example: Applying Intelligence to Determine Risk Rating**

Figure 18 illustrates the outcome of applying ratings for the Exploitability Index.

Figure 18. Example of the Exploitability Index

<table>
<thead>
<tr>
<th>Security Bulletin</th>
<th>Vulnerability Identifier</th>
<th>Exploitability Index assessment</th>
<th>Microsoft severity rating</th>
<th>Risk rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSYY-001</td>
<td>CVE-20YY-AAAA</td>
<td>1 - Consistent Exploit Code Likely</td>
<td>Critical</td>
<td>...</td>
</tr>
<tr>
<td>MSYY-002</td>
<td>CVE-20YY-BBBB</td>
<td>1 - Consistent Exploit Code Likely</td>
<td>Critical</td>
<td>...</td>
</tr>
<tr>
<td>MSYY-003</td>
<td>CVE-20YY-CCCC</td>
<td>1 - Consistent Exploit Code Likely</td>
<td>Important</td>
<td>...</td>
</tr>
<tr>
<td>MSYY-004</td>
<td>CVE-20YY-DDDD</td>
<td>2 - Inconsistent Exploit Code Likely</td>
<td>Moderate</td>
<td>...</td>
</tr>
<tr>
<td>MSYY-005</td>
<td>CVE-20YY-EEEE</td>
<td>3 - Functioning Exploit Code Unlikely</td>
<td>Critical</td>
<td>...</td>
</tr>
</tbody>
</table>

In addition, other considerations that were mentioned in Figure 15 above could apply here. For example, suppose that MSYY-001 is a Remote Code Execution for Microsoft Visio® (2003 SP3, 2007 SP2, and 2010 RTM) and this organization
only has the Microsoft Office Visio Viewer, which the security bulletin lists as non-affected software. In this instance, IT pros should determine that security update MSYY-001 does not apply and cancel it for deployment (as shown in Figure 19). Therefore, when IT pros take into account this additional information for the risk assessment, they may choose a different prioritization for their risk rating.

Figure 19. Example of the risk rating system

<table>
<thead>
<tr>
<th>Security Bulletin</th>
<th>Vulnerability Identifier</th>
<th>Exploitability Index assessment</th>
<th>Microsoft severity rating</th>
<th>Risk rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSYY-001</td>
<td>CVE-20YY-AAAA</td>
<td>1 - Consistent Exploit Code Likely</td>
<td>Critical</td>
<td>High</td>
</tr>
<tr>
<td>MSYY-002</td>
<td>CVE-20YY-BBBB</td>
<td>1 - Consistent Exploit Code Likely</td>
<td>Critical</td>
<td>High</td>
</tr>
<tr>
<td>MSYY-003</td>
<td>CVE-20YY-CCCC</td>
<td>1 - Consistent Exploit Code Likely</td>
<td>Important</td>
<td>High</td>
</tr>
<tr>
<td>MSYY-004</td>
<td>CVE-20YY-DDDD</td>
<td>2 - Inconsistent Exploit Code Likely</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td>MSYY-005</td>
<td>CVE-20YY-EEE</td>
<td>3 - Functioning Exploit Code Unlikely</td>
<td>Critical</td>
<td>Low</td>
</tr>
</tbody>
</table>

What has changed is that MSYY-001 is eliminated from the rating altogether because the customer does not have the affected software. Also, MSYY-005 was initially assessed as high priority because it was rated as Critical, but it has now been reprioritized downward. Conversely, MSYY-003 was given low priority before, but its priority has now been increased. In these cases, the changes reflect the additional information provided in the steps in Figure 15. The Exploitability Index helps here because, even though MSYY-003 is of lower severity than MSYY-005 (Important versus Critical), the fact that MSYY-003 is deemed likely to have consistent exploit code increases its overall priority. Conversely, the fact that MSYY-005 is deemed unlikely to have consistent exploit code decreases its overall priority.

If the outcome of this review determines that the security release is of low risk to the organization, the update can be passed to the standard update process and deployed when the necessary test and change request process has been completed. This guide discusses details of these stages later.

**Security Update Deployment Considerations**

There are a few final considerations in the Evaluate Risk stage of an IT pro’s risk-
management framework. Before the security updates have final approval for deployment, there may be additional considerations to ensure that a security update is not likely to introduce problems into an existing infrastructure. These factors do not affect the assigned risk rating of the security updates. However, it is important that IT pros consider these factors when they review the potential impact on systems and services within the production environment. To establish the category of the change request, IT pros should review several additional considerations, which are included in Figure 20.
Figure 20. Deployment considerations for security updates

<table>
<thead>
<tr>
<th>Security Update deployment consideration</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine whether there are any known issues or side-effects with the update that might delay or complicate the deployment.</td>
<td>Microsoft subjects all security updates to extensive research, development, and testing processes. Security updates are only released when they meet an appropriate level of quality. However, as part of the risk assessment process, administrators often want to identify any known issues. Review the “Known Issues” section of the security bulletin, which is in the “General Information” section at the top of each security bulletin. Typically, if there is an issue, it will point to a Knowledge Base article for the security bulletin at support.microsoft.com. IT pros can also search Knowledge Base articles by using the Search By KB Article Number tab on <a href="http://www.microsoft.com/technet/security/current.aspx">www.microsoft.com/technet/security/current.aspx</a>. Knowledge Base articles accompany all security bulletins and advisories. These articles include caveats or issues with security updates and, in addition, support engineers document common concerns from customers. Customers can also call Microsoft Customer Support if they have questions on any known issues with specific security updates.</td>
</tr>
<tr>
<td>Determine how many systems need the security update and what role those computers have (that is, how critical they are to the business).</td>
<td>The significant element here is not how many computers are affected, but how critical those computers are to the business. Key assets should be targeted to receive security updates first. Among other considerations, answering this question also helps to lessen the perceptible impact to users of certain critical business systems and determine the possible impact on network bandwidth in addition to the potential loading on update servers.</td>
</tr>
<tr>
<td>Security Update deployment consideration</td>
<td>Details</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Determine whether the size of the update is likely to impact the network infrastructure.</td>
<td>Deploying a large software update simultaneously to many computers can degrade network performance and adversely affect the proper operation of the network. IT pros should closely review all security update documentation and always be aware of the security update's size and the number of computers that will receive it. This information can also assist with properly scheduling the release. IT pros can find the file size of security updates by using the Microsoft Update Catalog service at catalog.update.microsoft.com and performing a query on the security bulletin number.</td>
</tr>
<tr>
<td>Check whether there are any company holidays or events that could hinder the deployment of the update.</td>
<td>Research has shown that some developers of malicious software have started targeting releases just before major holidays to maximize the potential that an update is not deployed before they can exploit it. For this reason, IT pros should be able to escalate high risk deployments, even over periods that would normally be holidays.</td>
</tr>
<tr>
<td>Ensure that enough resources are available to deploy the update or deal with any issues that users might experience during deployment.</td>
<td>IT pros should check the current status of the deployment team and make sure that the required individuals can be assembled to ensure that the update is completed within the required timelines.</td>
</tr>
<tr>
<td>Determine which deployment mechanisms will be required to deploy to all of the update targets.</td>
<td>Depending on the scope of the update, IT pros may need to use various mechanisms to deploy the update to all systems in the organization. For example, some IT pros may decide that mission-critical servers must be updated by some form of manual process to ensure that the service disruption is kept to a minimum. Other IT pros may determine that client computers can be updated by an automated deployment process by using WSUS. It is important that all required mechanisms are determined at this stage to ensure that the true impact of the update process is assessed.</td>
</tr>
</tbody>
</table>

**Note:** The organization’s overarching security update approach should have already covered much of this determination. However, it is still helpful to consider this step again prior to deployment.
<table>
<thead>
<tr>
<th>Security Update deployment consideration</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will additional changes be needed to support the deployment of the update?</td>
<td>If, for example, the security update applies only to the current service pack, and that service pack is not installed on certain production systems, it may not be possible to protect those systems against a particular security vulnerability. In this case, the impact and the category of the change request would be greater because both the service pack and the software update would need to be deployed.</td>
</tr>
<tr>
<td>Security Update deployment consideration</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Can you uninstall the update after it has been installed? | This is discussed in more detail later in this guide. However, when evaluating an update, determine whether it can be easily uninstalled if it causes a problem that is not identified during testing. Functionality for uninstalling updates can vary from fully automated uninstallation support to manual uninstallation procedures to no uninstallation. If an update cannot be uninstalled, the only option might be to restore the computer from a recent backup. Regardless of the uninstallation method that is required for an update, IT pros should ensure that there is a defined rollback plan in case the deployment does not match the achieved in the test environment. 

IT pros might also want to verify that there are recent backups of all computers that will be updated, and that these systems can be restored if the update cannot be successfully removed. An update is unlikely to cause systems to fail completely and require them to be restored from backup, but it is a circumstance that IT pros should be prepared to handle. 

Microsoft provides security update removal information in each security bulletin. Go to the “Security Update Deployment” section of the security bulletin and look up the “Removal Information” row in the table that relates to the relevant software. See www.microsoft.com/technet/security/current.aspx. |
It is also important that IT pros clearly define the technical details of the vulnerability. Specifically, IT pros need to make clear which operating systems, server roles, features, services, and applications are affected. The system management team can then use this information to determine the exact deployment plan across the organization.

After IT pros have successfully considered all of these steps, they should be in a position to determine whether the release needs to be deployed. If it does, they should be able to decide whether to follow the standard update timeline for all systems or whether the situation is urgent enough to require an expedited timeline (see "Stage 4: Deploy Updates," beginning on page 59, for details). The deployment phase may take some time, so we recommend that IT pros consider options for a short-term mitigation, which are discussed in the next stage of the customer risk-management framework.

### Stage 3: Evaluate Mitigation

**This section covers:**

- Mitigations and workarounds as a suitable short-term defense.
- Microsoft Active Protections Program (MAPP), which provides enhanced defenses while deploying security updates.

**At the end of this section, IT pros should:**

- Understand the differences between a mitigation and workaround:
  - For the purposes of this guide, a *mitigation* is a step that is taken at a network or system level to lower the risk that results from a vulnerability. A *workaround* is a modification in behavior at a user level.
  - Microsoft security bulletins and security advisories refer to mitigations as a setting, common configuration, or general best practice, which exists in
a default state, that could reduce the severity of exploitation of a vulnerability.

- Microsoft security bulletins and security advisories refer to workarounds as a setting or configuration change that does not correct the underlying vulnerability, but would help to block known attack vectors before applying the update.
- Find Microsoft resources that help to determine whether to implement a short-term mitigation.
- Understand that mitigations and workarounds are short-term defenses and that they are never intended to replace the deployment of security updates.
- Check the MAPP partner page to determine whether a MAPP member has provided an updated protection while deploying Microsoft security updates.
- Remember that they may need to remove the short-term mitigation after deployment of the Microsoft security update.

Microsoft resources referenced in this section:

- **Microsoft security bulletins (mitigations and workarounds).** Search security bulletins for specific information about mitigations and workarounds at [www.microsoft.com/technet/security/current.aspx](http://www.microsoft.com/technet/security/current.aspx). Mitigation and workaround information is contained in the “Vulnerability Information” section in each security bulletin.
- **Microsoft Active Protections Program (MAPP) partner page.** Determine whether active protections are available from security software providers at [www.microsoft.com/security/msrc/collaboration/mapppartners.aspx](http://www.microsoft.com/security/msrc/collaboration/mapppartners.aspx).
- **Microsoft Security Research & Defense blog.** This blog sometimes contains additional information about mitigations and workarounds. See [blogs.technet.com/srd/](http://blogs.technet.com/srd/).

---

**A Viable Short-Term Security Control**

**Implementing a short-term defense.** After IT pros have received the security notifications from Microsoft, and while they are performing the risk analysis, many choose to implement a defense to help prevent against attack. Depending on the risk rating and urgency, some organizations may implement the security update on the affected systems via an urgent update process (this is discussed later in this guide). However, in many cases, it is possible to implement viable short-term solutions. This gives IT pros more time to perform detailed risk analysis and deploy the security update via a standard update process. For example, if a vulnerability is found in a service that uses a particular port
number, which is not important to the operation of the systems in the 
organization, it might be easy to instigate a change to the firewall policies of the 
systems for the short term. This mitigation can offer a solution that will protect 
IT pros in the short term and afford them more time to perform a more thorough 
risk analysis before they fully deploy the security update.

In other cases, such as a Microsoft security advisory, a security update is often 
not available. Therefore, a suitable short-term defense is to follow the suggested 
workaround action in the Microsoft security advisory.

**Microsoft provides mitigations and workarounds.** As part of the process 
of investigating vulnerability reports, Microsoft identifies both mitigations and 
workarounds that help to protect against attempts to exploit the vulnerabilities 
that the security update addresses. When Microsoft identifies viable mitigations 
and workarounds for a specific vulnerability, this information is made available 
in the “Vulnerability Details” section of the security bulletin. If Microsoft cannot 
identify a viable mitigation or workaround, this is noted instead. Similarly, 
workaround information is contained in the “Suggested Action” section of the 
security advisory.

A mitigation, or mitigating factor, is a default setting, common configuration, or 
general best practice that could reduce the exploitation severity of a vulnerability, 
without typically requiring additional action. For example, for a vulnerability that 
can only be exploited if an obscure TCP port is open to the Internet, following 
commonly accepted best practices for enterprise firewalls would be a mitigating 
factor, because the firewalls typically close such ports by default. While a 
mitigation does not eliminate or address a vulnerability, it does introduce barriers 
to successful exploitation. The more mitigations a customer is able to take 
advantage of, the more obstacles an attacker would have to overcome to 
successfully use the vulnerability in an attack.

A workaround refers to a setting or configuration change that can be implemented 
to block known attack vectors before the associated security update can be 
applied. (The same factor or setting can be a mitigating factor for one customer 
and require a workaround for another. For example, if the TCP port mentioned 
in the previous paragraph is open, closing it would be a workaround.) 
Workarounds may not be feasible for everyone. They should be considered and 
evaluated against functionalities and operational considerations that may be 
identified as not relevant or needed in a particular computing environment.

In addition to presenting customers with additional information that can be used 
to assess risk and prioritize update deployment, mitigations and workarounds 
also allow customers to explore interim alternatives to deploying security updates 
or to provide additional protection while the update and deployment process is 
derway. The more mitigations and workarounds customers have at their 
disposal, the more options and information they can take advantage of to 
mitigate that overall risk.

In many cases Microsoft provides an automated “Fix-It” solution which 
automatically implements the mitigation or workaround. These Fix-Its may be

56
deployable via mechanisms such as Group Policy, allowing administrators to widely deploy mitigations across enterprises. For more information on Fix-Its see support.microsoft.com/fixit.

**Mitigations and workarounds never replace security updates.** The goal in providing mitigation and workaround information for specific vulnerabilities in security bulletins is to give IT pros an option that they can use to protect the environment immediately; that is, while the security update is undergoing the appropriate testing before being broadly deployed. Just as mitigation information is never intended to justify not applying security updates, workaround information is provided as an interim measure until the relevant security updates are applied. Therefore, mitigations should be viewed as being closely tied both to risk assessment and the deployment processes and procedures.

IT pros should consider implementing mitigations and workarounds immediately for issues identified as high risk to the environment so they can provide better protection while the security updates are applied. Issues for which no mitigations or workarounds are available may merit increased priority for deployment.

Figure 21 shows a summary of the steps that can be used to evaluate and deploy a short-term mitigation (or workaround) in an organization.

Figure 21. Evaluate Mitigation stage

The Evaluate Mitigation stage has only one consideration, which is *whether it is possible to implement an effective short-term mitigation faster than it is possible to deploy the security update*. If there is a short-term mitigation that can be used, this should be documented and implemented as quickly as possible. To aid in determining the possibility of using a mitigation, IT pros can use several resources that are documented in Figure 22.

Figure 22. Mitigation evaluation resources
<table>
<thead>
<tr>
<th>Mitigation evaluation resources</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the security bulletin or advisory to determine whether there are any mitigations or workarounds in your organization that might alleviate the short-term risk.</td>
<td>In security bulletins, mitigation and workaround details are provided for each specific vulnerability in the “Vulnerability Information” section of the bulletin. IT pros should reference two areas in particular: Mitigating factors refer to a setting, common configuration, or general best practice, which exists in a default state, that could reduce the severity of exploitation of a vulnerability. Workarounds refer to a setting or configuration change that does not correct the underlying vulnerability, but would help to block known attack vectors before applying the update. Microsoft has tested the listed workarounds and typically states in the discussion whether a workaround reduces functionality. In security advisories, most contain a “Suggested Actions” section, which, in turn, contains a section called “Workarounds.” Again, these are workarounds that Microsoft has tested. Although these workarounds will not correct the underlying vulnerability, they will help block known attack vectors. When a workaround reduces functionality, it is identified in this section.</td>
</tr>
</tbody>
</table>

| Determine whether there are any active software security protections that can be used to help mitigate the vulnerability. | Microsoft Active Protections Program (MAPP) is a program for security software providers. Members of MAPP receive vulnerability information early so that they can provide updated protections to IT pros via their security software or devices, such as antivirus software, network-based intrusion detection systems, or host-based intrusion prevention systems. Upon receipt of the Microsoft security bulletin summary, or while they are performing the risk analysis, IT pros are encouraged to check the MAPP partner page for up-to-date active protections at www.microsoft.com/security/msrc/mapp/partners.mspx. The MAPP program includes many global organizations whose businesses span numerous security segments (for example, intrusion detection, intrusion prevention, antivirus software, and so on). The MAPP partner page includes links to the active protections that should be applied during the risk-management process. The result for IT pros and organizations is enhanced protections while they deploy Microsoft security updates. For more information about active software security protections, see www.microsoft.com/security/msrc/collaboration/mappfaq.aspx or reference the Appendix. |
Mitigation evaluation resources | Details
--- | ---
Check the Microsoft Security Research & Defense blog to determine whether any additional information is available to help mitigate the vulnerability. | As mentioned above in the “Stage 2: Evaluate Risk” section of this guide, the Security Research & Defense blog contains specific technical information about additional mitigations and workarounds that are not contained in security bulletins or advisories. This blog is available at blogs.technet.com/srd/.

Although the MSRC blog is a valuable Microsoft security resource, it does not focus on providing IT pros with mitigations or workarounds. In contrast, bloggers on the Security Research & Defense blog are individuals from Microsoft who perform in-depth technical analysis of vulnerability reports. These individuals investigate and perform research on new vulnerabilities, and provide technical guidance for security bulletins, including information about the mitigations and workarounds that are referenced in the bulletins. They also ensure that updates are effective in eliminating software vulnerabilities.

**High risk but no mitigation.** If the security update is determined to be high risk, but no effective mitigation is found, the best course of action is to initiate an urgent update to all affected systems in the organization.

**Remove the short-term mitigation or workaround.** When the short-term mitigation is fully in place, IT pros can use the standard update process to deploy the update. When the deployment has been confirmed as part of the monitoring process, the short-term mitigation can be removed if it is desirable to help restore the normal organization's normal operations (unless, of course, this is an active protection from MAPP).

**Stage 4: Deploy Updates**

**This section covers:**
- The Deploying Microsoft Windows Server Update Services guide.
- Using the security update deployment timeline with standard-priority and high-priority updates.
- The six steps to deploying a security update:
  1. Plan the deployment.
  2. Determine whether the security update is available for download.
  3. Obtain the required update files.
  4. Create the update package.
  5. Test the package.
6. Deploy the package to systems that require it.

At the end of this section, IT pros should:

- Read the Deploying Microsoft Windows Server Update Services guide to understand the options for configuring WSUS to the organization’s network topology. This is very important.
- Understand the six steps and the various resources for deploying a security update.
- Understand the considerations to balance the need to deploy a security update quickly versus conducting more thorough testing.
- Understand where and how to obtain the security update files.
- Understand the need to carry out a minimum level of testing to show that:
  - When the installation is complete, the computer will restart as it is designed to.
  - The security update, if it is targeted at computers that are connected across slow or unreliable network connections, can be downloaded across these links. When the download completes, the security update should successfully install.
  - The security update is supplied with an uninstall routine, which can be used to successfully remove the update, if required.
  - Business-critical systems and services continue to run after the security update has been installed.

Microsoft resources referenced in this section:

- **Windows Server Update Services (WSUS) and Updates.** This page helps explain how WSUS stores and manages Microsoft updates. See technet.microsoft.com/updatemanagement/bb245780.aspx.
- **The Deploying Microsoft Windows Server Update Services guide.** See go.microsoft.com/fwlink/?LinkId=161140.
- **The Windows Update Agent (WUA) application programming interface (API).** See “Searching, Downloading, and Installing Updates” and “Searching, Downloading, and Installing Specific Updates” on the MSDN website for scripts that can be used to further customize security updating. Create and change windows, orchestrate complex update workflows on server farms, or automatically update newly provisioned machines:
  - **WUA API.** See msdn.microsoft.com/library/aa387099(VS.85).aspx.

Local Publishing. The WSUS API allows IT pros to create and publish custom updates, applications, and device drivers for their organizations through a process called local publishing. Local publishing is best performed by organizations that have dedicated development and testing resources, because the planning, implementation, testing, and deployment of custom updates is a complex and time-consuming process.

Note: The WSUS APIs are very complex to use for anyone other than a professional developer. Further, it is important to understand that WSUS does not support non-Microsoft updates and for this need, Microsoft recommends that IT pros use Microsoft System Center Configuration Manager or have professional developers build the equivalent functionality on top of the public WSUS APIs.

The local publishing process is divided into seven separate steps on the following web page: msdn.microsoft.com/library/bb902470(VS.85).aspx.

Microsoft Download Center. See www.microsoft.com/download/.


Microsoft Baseline Security Analyzer (MBSA). This tool helps small and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Use MBSA to detect common administrative vulnerabilities and missing security updates on computer systems. MBSA does not perform the installation of updates; it only scans for updates and has the ability to configure the computer to use Microsoft Update for update management. See technet.microsoft.com/security/cc184924.aspx.

Microsoft System Center Configuration Manager. Another solution from Microsoft that provides additional features that MBSA, WSUS, and others do not provide. See www.microsoft.com/systemcenter/configurationmanager/.

Microsoft Customer Service & Support (CSS). Contact CSS either through your organization’s existing Microsoft support contacts or by calling (1) (866) PC-SAFTETY [(1) (866) 727-2338 in the United States and Canada.] Internationally, IT pros should contact their local Microsoft subsidiary. See support.microsoft.com/common/international.aspx.

---

MBSA is localized into four languages: English, German, French, and Japanese but the underlying detection accurately scans target computers in any language that Microsoft Update and WSUS support.
The Deploying Microsoft Windows Server Update Services Guide

The first step in this stage is to read and fully understand the Deploying Microsoft Windows Server Update Services guide. This guide describes how to deploy WSUS and includes a comprehensive description of how WSUS functions. It also includes descriptions of WSUS scalability and bandwidth management features. In addition, this guide offers IT pros step-by-step procedures for installation and configuration of the WSUS server. Sections include how to update and configure Automatic Updates on client workstations and servers that WSUS will update. For more information, see technet.microsoft.com/library/cc720507(WS.10).aspx.

Standard and Urgent Deployments

As this guide discussed earlier, an organization can usually follow one or more deployment processes, depending on the installation infrastructure and the urgency of the update. For low-risk vulnerabilities, IT pros can follow the standard update timeline documented in this guide to ensure that the update is deployed in a manner that minimizes the cost and disruption to the organization. For vulnerabilities that pose a particularly high risk to the organization, IT pros should consider using an abbreviated version of this timeline that focuses on a rapid deployment above other considerations.

Phases of this stage. The steps and duration of the aforementioned timelines depend on the organization's staffing and service-level agreements (SLAs) for various classes of systems and the deployment processes that are used. However, the three basic phases of these deployment processes usually remain the same:

- **Create.** The process that is required to obtain the security update binaries and package them so they are ready to be deployed to the target computers in the organization.

- **Test.** The process of testing the impact of the security update package on test systems that emulate the range of server or client systems in the organization.

- **Deploy.** The process of installing the security update packages on the required computer systems. This step should also include a reporting or monitoring phase to ensure that the status of the systems can be tracked as the deployment is rolling out.

Standard Package Application Process

Maximum end-to-end process timeline of one month. The goal of the standard package application process is to deliver the security update into the production environment in a manner that minimizes the disruption to the organization’s users and services. At the same time, it should ensure that the lower-priority security updates are deployed before the next round of security updates are published. This typically sets a maximum end-to-end process timeline of one
month (the typical duration of the standard Microsoft security update release cycle). Figure 23 shows a summary of the steps involved in the Standard Update Timeline.

Figure 23. Standard update timeline

**Six steps to deploy an update.** IT pros should take six steps when planning the deployment of a new security update:

1. Plan the deployment.
2. Determine whether the security update is available for download.
3. Obtain the required update files.
4. Create the update package.
5. Test the package.
6. Deploy the package to systems that require it.

**Planning the Deployment**

Deployment is the process of implementing the protection provided by the security update. Deployment is the ultimate goal of the process, so understanding the deployment methods that are available and factoring them into your assessments are as important as a security risk assessment.

In this step, IT pros should understand the possible deployment methods and thereby create a plan for deploying the security updates. It is important to understand how the possible deployment methods may impact a schedule and make any necessary changes. For example, if WSUS does not support a security update, and that is a primary deployment method, it may be determined that it will take two days longer to deploy the update than originally planned. In turn, IT pros may decide to implement workarounds to provide necessary protections during this deployment window.

**Check the security bulletin.** Additional information about deployment methods is contained in the security bulletin in the section: “Update Information—Detection and Deployment Tools and Guidance.” During this stage, it is helpful to use the WSUS built-in reporting facility to see whether systems require any security updates.

**Plan deployment in parallel with the other steps.** Throughout the planning deployment step, some progressions are intricately interrelated and not necessarily linear. In some organizations, steps occur simultaneously, whereas in
others, they are sequential. IT pros should decide on the implementation of these steps based on the policies, needs, and resources of their organization. The most important thing for these steps is not the specific structure and order, but rather that these different stages can inform and respond to one another. The key for any implementation is to remain flexible and adaptable, and determine an achievable deployment plan (an example is shown in Figure 24 below) that takes into consideration the requirements of the updates and the limitations of the IT infrastructure. Using the information that was provided at the risk evaluation stage, the deployment team needs to quickly determine which systems need to be updated and in what order.

**Quick deployment versus thorough testing.** IT pros might have a clear understanding of which updates need to be rolled out quickly and which ones can be subjected to a more thorough testing process, or the distinction may be less clear. IT pros need to determine exactly how many systems are affected by the security updates and then set a timeline for the updates that meets the organization's SLAs for each system. It is recommended that organizations have a policy to help address this problem.

To address this challenge, IT pros should roll out the security updates based on the organization's policy regarding the need to get the security updates deployed quickly versus the need to test them in the environment, which is discussed later in this guide. Some organizations divide systems into target groups based on how IT pros want to deploy security updates. Many organizations use separate groups for desktop computers and servers. Many also create a group of “test” machines to perform early deployment testing of new security updates. In WSUS, the grouping structure is quite flexible, as computers can belong to multiple groups, such as desktop and test.

This concludes the planning stage. At this point, IT pros should have a schedule that reflects all elements of the assessments and planning regarding security risk, including risk rating of the security updates, mitigations, and workarounds, as well as testing and deployment.

**Example: Planning Security Update Deployment**

Deployment planning can be a complex process because the scope of the update could range from a single system to every system in the organization. IT pros may be unlikely to have an update system that can handle a simultaneous update of all systems in the organization, so the deployment team needs to determine how many systems can be supported, and at what time.

For example, if an organization has an update system that can support 500 systems at one time and a designated high risk update is required for 5,000 systems, the organization will have to space the deployment to avoid overloading the update servers. Most organizations should have already identified priorities for systems in the organization. Typically, there are at least two priority levels; sometimes, these are referred to as “High Value (HV)” and “Standard” or “General” systems. These priorities are then applied to both the server and client
computers, giving a total of four system categories. You can then use these definitions to help stage the deployment by selecting systems from one or more of these groupings up to the limit of the deployment system. In our example, the deployment team determined that the systems should be categorized as shown in Figure 24.

Figure 24. Example of a security update deployment plan

<table>
<thead>
<tr>
<th>System category</th>
<th>Total systems</th>
<th>Total at risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HV Servers</td>
<td>50</td>
<td>20</td>
<td>Server computers that provide mission-critical services to the organization including production or revenue-earning systems.</td>
</tr>
<tr>
<td>General Servers</td>
<td>200</td>
<td>180</td>
<td>Server computers that provide infrastructure services and support functions. Although these devices are important, they do not directly contribute to the organization’s revenue streams.</td>
</tr>
<tr>
<td>HV Clients</td>
<td>2,000 (1,500 remote*)</td>
<td>1,000 (800 remote*)</td>
<td>Systems used for functions in the organization that are determined to have an increased importance to the organization. This could be due to the role of the computer user or due to the sensitivity of the data and applications stored on the systems.</td>
</tr>
<tr>
<td>General Clients</td>
<td>4,500 (2,000 remote*)</td>
<td>1,400 (600 remote*)</td>
<td>Systems that provide various services to the organization, but do not store sensitive information.</td>
</tr>
</tbody>
</table>

*In this context, “remote” refers to remote portable computers.

In Figure 24, note that client systems are also identified by the number of remote portable computers that are included. This information can be important for some vulnerabilities because remote systems may be exposed to attack outside the protections (and possible mitigations) of the organization’s network edge (for example, a network firewall). In cases like this, it may be necessary for the deployment plan to prioritize remote general clients above other fixed systems if this additional exposure significantly increases their risk of attack.

Using this information, it is possible to build an example deployment plan that takes into account the real-world capabilities of the deployment infrastructure. In this example organization, the SLA for an urgent update on all systems is that the update is delivered within 24 hours, as shown in Figure 25.
In this example, the deployment process is running very close to its maximum for this number of supported systems. If an additional 500 systems had needed security updates, the organization would not have been able to meet the urgent SLA for all of these systems. As part of the ongoing systems management process, it is important that the deployment team evaluates the maximum update capabilities of its deployment system and ensures that, in a worst-case scenario, the organization’s SLAs are met for each system category.

**Is a Security Update Available for Download?**

The next step in the Standard Update Timeline is to obtain the necessary security update files. For most monthly Microsoft security update release cycles, the security update files are available at the same time as the security bulletin summary’s release. In some situations, the security update files take a brief amount of time to propagate through Microsoft services. If IT pros cannot access the Microsoft security update after it has been released, they should contact Microsoft CSS, either through the organization’s existing Microsoft support contacts or by calling (1) (866) PC-SAFETY [(1) (866) 727-2338 in the United States and Canada.] Internationally, IT pros should contact their local Microsoft subsidiary. See support.microsoft.com/common/international.aspx.

In the case of security advisories, a security update is only included if the advisory requires it. Therefore, IT pros should refer to the advisory itself to

---

**Figure 25. Deployment phases**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Timing</th>
<th>System Categories</th>
<th>Total</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>08:00–12:00</td>
<td>HV Servers, General Servers, and HV Clients (first phase)</td>
<td>500</td>
<td>20 HV Servers, 180 General Servers, 300 HV Remote Clients</td>
</tr>
<tr>
<td>2</td>
<td>12:00–16:00</td>
<td>HV Clients</td>
<td>500</td>
<td>500 HV Remote Clients</td>
</tr>
<tr>
<td>3</td>
<td>16:00–20:00</td>
<td>HV Clients and General Clients (first phase)</td>
<td>500</td>
<td>200 Remaining HV Clients, 300 General Remote Clients</td>
</tr>
<tr>
<td>4</td>
<td>20:00–00:00</td>
<td>General Clients</td>
<td>500</td>
<td>300 General Remote Clients, 200 Remaining General Clients</td>
</tr>
<tr>
<td>5</td>
<td>00:00–04:00</td>
<td>General Clients</td>
<td>500</td>
<td>500 General Clients</td>
</tr>
<tr>
<td>6</td>
<td>04:00–08:00</td>
<td>General Clients</td>
<td>100</td>
<td>100 General Clients</td>
</tr>
</tbody>
</table>
determine whether there is an accompanying security update that will need to be downloaded and deployed. If there is not an accompanying file for the advisory, upon completion of the applicable investigation, Microsoft advises the appropriate actions that IT pros should take to protect the organization’s computer systems.

**Obtaining the Required Security Update Files from a Trusted Source**

Regardless of when the files are released, IT pros can obtain the security update files from several sources, which include:

- Microsoft security bulletins.
- Microsoft deployment tools, such as Microsoft Update, Windows Update, WSUS, or System Center Configuration Manager.

*Note:* Often, IT pros use Microsoft detection and deployment tools to obtain security updates, yet cannot find the security updates. It is possible that new software has been recently added and the respective tool has not been updated to reflect the new software.

- The Microsoft Download Center. See [www.microsoft.com/download/](http://www.microsoft.com/download/).
- The Microsoft Update Catalog service. See [catalog.update.microsoft.com](http://catalog.update.microsoft.com).

For this section, the guide will use the Microsoft Update Catalog service. This is a service from Microsoft that provides a listing of updates that can be distributed over a corporate network. Microsoft Update supports updates as MSIs (MSPs or MSUs included), update.exe executables, and other file formats. Most of the security updates are incorporated into a .cab file. IT pros can also use the Microsoft Update Catalog service as a one-stop location for finding other Microsoft software updates, drivers, and hotfixes.

To download updates by using the Microsoft Update Catalog service, follow these steps:

1. **Step 1:** Access the Microsoft Update Catalog service at [catalog.update.microsoft.com](http://catalog.update.microsoft.com). To view a list of frequently asked questions about Microsoft Update Catalog, see [catalog.update.microsoft.com/v7/site/Faq.aspx](http://catalog.update.microsoft.com/v7/site/Faq.aspx).

2. **Step 2:** Search for updates in the Microsoft Update Catalog:
   - In the Search box, type your search terms. For example, you might type **Windows 7 Security**
   - Click Search, or press Enter.
   - Browse the list that is displayed to select the updates to download.
   - Click Add for each selection to add it to the download basket.
   - To search for additional updates to download, repeat the steps above.
Step 3: Download updates from the Microsoft Update Catalog:

- Under the Search box, click view basket to view the download basket.
- Verify your list of updates, and then click Download.
  Note: If prompted, review the license agreement and then click Accept to accept.
- In the Download Options window, in the Folder box, select the location where you want to save the updates. Either type the full path of the folder, or click Browse to locate the folder.
- Click Continue to start the download.
- When the download is complete, click Close to close the Download Results window.
- Close the Microsoft Update Catalog window.
- Find the folder location that was specified earlier in this step.
- Double-click each update, and then follow the instructions to install the update.
  Note: If the updates are intended for another computer, copy the updates to that computer, and then double-click the updates to install them.
- If all of the items that were added to the download basket are installed successfully, this step is finished.

Using this site, IT pros can search for updates and build a list of the required updates for each of the operating systems that they need to support. IT pros can then download the required files and use them to build the deployment packages for the deployment process.

Creating Update Packages

There are several approaches to choose from to build the update package for your organization. Depending on the organization’s management infrastructure, the update package type, and the operating systems or applications that require the update, multiple update packages may need to be created.

WUA API. The WUA API is a set of Component Object Model (COM) interfaces that enable system administrators and programmers to access Windows Update and WSUS. It is possible to write scripts and programs to examine which updates are currently available for a computer, and then install or uninstall updates. System administrators can use WUA to programmatically determine which updates to apply to a computer, download those updates, and then install them with little or no user intervention. ISVs and developers can integrate WUA features into computer management or update management software to provide a seamless operating environment.

For more information about using the WUA API, see
Local Publishing. The WSUS API enables IT pros to create and publish custom updates, applications, and device drivers for their organization through a process called local publishing. Local publishing is best performed by organizations that have dedicated development and testing resources because the planning, implementation, testing, and deployment of custom updates is a complex and time-consuming process.

Note: The WSUS API is complex to use for anyone besides a pro developer and does not support non-Microsoft updates. For this requirement, Microsoft recommends that IT pros use System Center Configuration Manager or hire professional developers to build the equivalent functionality on top of the public WSUS API.

For more information about local publishing, see msdn.microsoft.com/library/bb902470(VS.85).aspx. The local publishing process consists of seven steps:

1. Set up the update server and clients to trust locally published updates.
2. Create the update binary (an MSI or MSP package, or an executable file).
3. Create the update metadata, specifying when and how the update should be installed.
4. Publish the update to the update server.
5. Test the update by deploying it to a set of test clients.
6. Deploy the update to all clients.
7. Revise and version the update.

For more information about this process, see the following topics:

- “Revising and Versioning Updates” at msdn.microsoft.com/library/bb902492(VS.85).aspx.

Sample scripts. Microsoft also provides WSUS sample scripts. For the WSUS sample script repository see www.microsoft.com/technet/scriptcenter/scripts/sus/default.mspx?mfr=true.

Advertisements by using System Center Configuration Manager. After IT pros have defined programs for a package and the package data has been sent to one or more distribution points, IT pros who are using Configuration Manager to manage the deployment process can create advertisements that make those
programs available to the clients in the specified collection. For more information about advertisements, see “About Advertisements” at technet.microsoft.com/library/bb694110.aspx.

Testing Update Packages

- As explained in "How Microsoft Tests Security Updates" on page 16, Microsoft subjects security updates to extensive testing in real-world conditions before releasing them to the public, so security updates that cause disruptions to ordinary production environments are uncommon. Nevertheless, every IT environment is different, so IT pros should run update packages through some acceptance testing to ensure that business-critical systems will continue to run successfully after the security update has been deployed. Administrators, together with business representatives, should create a set of tests that are performed however critical the security update. IT pros should always perform a minimum level of testing to show that:
  - When installation is complete, the computer will restart as designed.
  - The security update, if it is targeted at computers that are connected across slow or unreliable network connections, can be downloaded across these links. When the download completes, the security update should successfully install.
  - Business-critical systems and services continue to run after the security update has been installed.
  - Before deploying the security update into production, information is collected about any troubleshooting steps, procedures, and tools used during testing, and any uninstallation routines that can be used to successfully remove the software update if required. This information should be made available to service desk support staff and the operations team.

No matter how much testing is performed, rolling out a security update into production often produces effects that might never be anticipated or replicated in a lab environment. After applying an update or group of updates to test computers, test all applications and functionality. The amount of time and expense that IT pros dedicate to testing the update should be determined by the potential damage that a problematic update deployment would cause.

IT pros can test an update in two ways:

1. In a test environment.
2. In a pilot deployment.

Test Environment

A test environment can consist of a test lab and include plans that detail what should be tested and the cases to describe how each component is tested. Organizations that have the resources to test updates in a test
environment should always do so because it may reduce the number of problems that update incompatibility with applications could cause. Even if an organization does not have the resources to test security updates, IT pros should always test service packs before they deploy them to production computers.

**Benefits of a test environment.** The test lab can consist of a single lab or several labs, each of which supports testing without presenting risk to the product environment. In the test lab environment, members of the testing team can verify deployment design assumptions, discover deployment problems, and improve the understanding of the changes that specific updates implement. Such activities reduce the risk of errors occurring during deployment and enable members of the test team to rapidly resolve problems that might occur while they deploy an update or after they apply an update.

Many organizations divide their testing staff into two functional groups: the design team and the deployment team. The design team collects information that is vital to the deployment process, identifies immediate and long-term testing needs, and proposes a test lab design (or recommends improvements to the existing test lab). The deployment team completes the process by implementing the design team’s decisions and testing new updates on an ongoing basis.

Early in the update test environment, the deployment team tests the update deployment process to validate that the design is functional. Later, after IT pros have identified an update to deploy, the deployment team tests the individual updates to ensure that all of them are compatible with the applications that the organization uses.

**Equal representation.** An update test environment should have computers that represent each of the major computer roles in the organization, including desktop computers, mobile computers, and servers. If the computers for each role have different operating systems, each operating system should be available on dedicated computers, on a single computer with a multiple-boot configuration, or in a virtual desktop environment.

After the deployment team has a set of computers that represents each type of computer in the organization, it can connect them to a private network. IT pros also need to connect test versions of the update infrastructure computers. For example, if IT pros plan to deploy updates by using WSUS, connect a WSUS server to the lab network.

IT pros should load every application that is used on the lab computers and develop a procedure to test the functionality of each application. For example, to test the functionality of Internet Explorer, IT pros could visit both the Microsoft website and an intranet website. Later, when IT pros are testing updates, they would repeat this test. If one of the applications fails the test, the update that is currently being tested might have caused a problem. (Subsequent sections in this guide have more information on testing updates.)
Pilot Deployment

In addition to testing the implementation of an update, conducting a pilot deployment provides an opportunity to test the organization’s deployment plan and the deployment processes. It helps IT pros to determine how much time is required to install the update, and the personnel and tools that are required. It also provides an opportunity to train support staff and to gauge user reaction to the update process. For example, if a particular update takes an hour for a dial-up user to download, IT pros might consider identifying an alternative method to deliver the update to the user.

Test Process Steps

After the pilot deployment, the next step is to run through a set of test use cases to determine whether the update has caused a change to any required functionality or features in the operating system or applications running on it. Figure 26 details the test process steps that IT pros should take.

<table>
<thead>
<tr>
<th>Test process steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>For all affected software updates: test security update installation and uninstallation.</td>
<td>These tests ensure that it is possible to successfully deploy and install the security update package on the target systems. Make sure that packages can also be rolled back if a compatibility issue is found.</td>
</tr>
<tr>
<td>For client and server updates: test post-update system functionality.</td>
<td>These tests ensure that the required local services on a system are still available and performing at the right level after the update has been applied.</td>
</tr>
<tr>
<td>For client and server updates: test network interfaces.</td>
<td>These tests ensure that the required remote services that are provided to the network via a specific interface system are still available and performing at the required level after the update has been applied.</td>
</tr>
</tbody>
</table>

If IT pros are testing a large number of applications, scripting can be identified to automate the testing of updates.
Test process steps | Details
--- | ---
For other security updates (for example, the Microsoft Office system, Internet Explorer, and so on): test user applications. | On client systems, it is important to test the functionality of the required business applications. These test cases are used to exercise a set of functionality for all of the supported user applications.

Later on, there are two example user application tests for the Microsoft Office system and Internet Explorer. IT pros need to identify and develop collections of repeatable tests for each critical business user application in their organization.

The next few sections of this guide provide some example user test cases that can be applied to test the functionality of the test process steps in Figure 26. **These steps are only a baseline to start the testing process. We recommend that IT pros modify them as needed to meet the organization’s specific requirements.**

**Test Security Update Installation**

Figure 27 describes some suggested steps for testing the installation and uninstallation of the security updates for all affected products.
### Figure 27. Test security update installation steps

<table>
<thead>
<tr>
<th>Installation steps</th>
<th>Details</th>
</tr>
</thead>
</table>
| **Pre-Installation** | Confirm that the update applies to the system, operating system, or application version. See “Stage 2: Evaluate Risk” in this guide for more information.  
Ensure that there are no noted caveats.                                                                                                                                                                                                                                                                                                                                                                      |
| **Installation**     | Check that the installation process executes and completes successfully, and ensure that no errors appear during this process.  
Review the system and update process logs (for example, %systemroot%\KB[XXXXXX].log, where KB[XXXXXX] refers to a specific KB article number; for example KB973346) and check that no errors are recorded.  
Check that update installation is correctly reported. Depending on the update, this might involve:  
- Checking the update installation key in the registry to ensure that it was properly created.  
- Checking that the update installation was correctly reported by the monitoring system.  
- Ensuring that the update appears in Control Panel, in the Add or Remove Programs folder.  
- Checking that the uninstallation directory exists and contains the changed binary files.  
- Testing that the system does not exhibit unusual or abnormal behavior.                                                                                                                                                                                                                                                                          |
| **Post-Installation**| Check that none of the specified changes have been reversed or altered.  
Check that the system does not exhibit unusual or abnormal behavior. Restart the system, manually if necessary.                                                                                                                                                                                                                                                                                                         |
| **Attempt to Reinstall Update** | Check that the update detects whether it has failed (partially installed) previously or the attempt to reinstall fails.  
Check that there are no changes to uninstallation parameters or binaries.                                                                                                                                                                                                                                                                                                                                                       |
Installation steps | Details
--- | ---
Uninstall | Check that the uninstallation process executes and completes successfully.
Check that all changes have reverted to the original configuration by checking registry keys, binaries, configuration files, and so on.
Check that no errors are posted in the system or update process logs (for example, %systemroot%\KB[XXXXXX].log).
Check that the update installation has been removed. Signs of success include:
- The registry key has been removed.
- The monitoring tool has correctly reported that the update is missing.
- The update does not appear in Control Panel in the Add or Remove Programs folder.
- The Uninstall directory is removed.
See the “Uninstalling Security Updates” section later for additional information about uninstalling updates.

Post-Uninstall Restart | Check that none of the specified changes have been reversed or altered.
Check that the system does not exhibit unusual or abnormal behavior.

Repeat installation and uninstallation tests with any required option switches and parameters. For example, test with a no restart option, a quiet option, and so on.

Test Post-Update System Functionality

Figure 28 and Figure 29 detail some suggestions for testing system functionality after the installation of security updates for servers and clients, respectively. Again, these steps are only a baseline to start the testing process. We recommend that IT pros modify these suggestions to meet their organization’s specific requirements.
Figure 28. Post-update system functionality tests for servers

<table>
<thead>
<tr>
<th>Server Usability Tests (Note: at the end of each test, check event logs for errors related to operation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test that the system completes a startup (cold boot) and restart (warm boot) successfully.</td>
</tr>
<tr>
<td>Log on as a local administrator and test that the logon completes successfully.</td>
</tr>
<tr>
<td>Ensure that all required services start correctly.</td>
</tr>
<tr>
<td>Network initialized properly</td>
</tr>
<tr>
<td>Check that the required ports are still enabled.</td>
</tr>
<tr>
<td>Ensure that the IP address, network mask, and other network parameters (for example, default gateway, DNS, and WINS) are assigned correctly.</td>
</tr>
<tr>
<td>Check that you can PING the localhost, a host on the local network (for example, the default gateway), and a host on a remote network segment (for example, an Internet-based Web server).</td>
</tr>
<tr>
<td>If a proxy is required, check access and the external host by using the proxy.</td>
</tr>
<tr>
<td>Domain Controller</td>
</tr>
<tr>
<td>Ensure that the domain controller passes all DCDIAG.EXE tests.</td>
</tr>
<tr>
<td>Check that clients can detect the domain controller (for example, the client can PING the host and perform “nslookup” after the ipconfig flushdns command).</td>
</tr>
<tr>
<td>Check that the Distributed File System (DFS) Replication and the File Replication Service (FRS) (if applicable) are working correctly.</td>
</tr>
<tr>
<td>DNS Server</td>
</tr>
<tr>
<td>Check that the DNS service starts and successfully completes both simple query and recursive test types.</td>
</tr>
<tr>
<td>Ensure that the naming service resolves names properly (for example, the ping servename command should return the server name and IP address).</td>
</tr>
<tr>
<td>WINS Server</td>
</tr>
<tr>
<td>Check that the WINS service is started and in a healthy state.</td>
</tr>
<tr>
<td><strong>Server Usability Tests (Note: at the end of each test, check event logs for errors related to operation)</strong></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Test that the WINS database consistency check completes successfully.</td>
</tr>
<tr>
<td>Ensure that WINS clients can resolve and renew names.</td>
</tr>
<tr>
<td>Check server event logs to make sure that they do not contain errors related to WINS operations.</td>
</tr>
<tr>
<td><strong>Dynamic Host Configuration Protocol (DHCP) Server</strong></td>
</tr>
<tr>
<td>Test that the DHCP service starts properly; that the Microsoft Management Console (MMC) DHCP snap-in server statistics show proper operations; and that the address database shows addresses that have been leased.</td>
</tr>
<tr>
<td>Ensure that DHCP clients can obtain IP addresses.</td>
</tr>
<tr>
<td>Run a DHCP database consistency check and ensure that it completes without errors.</td>
</tr>
<tr>
<td><strong>IIS Server</strong></td>
</tr>
<tr>
<td>Ensure that the IIS service is running, check services to see that the WWW Publishing service started properly, and check processes to see that the INETINFO.EXE process is running.</td>
</tr>
<tr>
<td>Verify that the IIS services start up after restart.</td>
</tr>
<tr>
<td>Check that the authentication and encryption levels on the Web server work properly (that is, users can access Web content that they are authorized to access).</td>
</tr>
<tr>
<td>Check that the IP address and domain name in IIS Management is set properly.</td>
</tr>
<tr>
<td>Check that the Root folder and all necessary Web files are present.</td>
</tr>
<tr>
<td>Test that clients can access both static and active Web pages on the server.</td>
</tr>
<tr>
<td><strong>File and Print Server</strong></td>
</tr>
<tr>
<td>Test that an administrator can create a new file share.</td>
</tr>
<tr>
<td>Check that an administrator can successfully change domain user access to file share.</td>
</tr>
<tr>
<td>Ensure that the client systems can locate the file share after it has been published in Active Directory®.</td>
</tr>
</tbody>
</table>
Server Usability Tests (Note: at the end of each test, check event logs for errors related to operation)

- Log on as an administrator and check that you can successfully add a new printer.
- Ensure that the client systems can access the printers after they are published in Active Directory.
- From a client system, ensure that you can successfully print a document.

Figure 29. Post-update system functionality tests for clients

Client Usability Tests (Note: at the end of each test, check event logs for errors related to operation)

Administrator Tests

- Check that a domain administrator user can join a workstation to a child domain.
- Ensure that a domain administrator user can log on, change a password, print, view and manage print queues, access files on a remote share, and release and renew an IP address.

User Tests

- Check that a domain user can log on, change his or her password, print, view print queues, and access files on a remote share.

Testing Application Interfaces

The next step in the test phase is to ensure that the required remote services and applications that were provided to the network via a specific interface system are still available and performing at the required level after the update has been applied. Figure 30 and Figure 31 list several suggested tests that IT pros can use to confirm the correct system functionality after the installation of the security updates. Again, these steps are only a baseline to start the testing process. We recommend that IT pros modify these steps to meet their organization’s specific requirements.

Figure 30. Local application tests
### Local Application Interfaces

**IIS Server**

- Check that you can authenticate to the local IIS service.

- Log on to an administrator account and check that you can perform the following tests:
  - Administer the local IIS service.
  - Retrieve a static page from the local IIS service.
  - Retrieve an ASP page from the local IIS service.

**SQL Server®**

- Check that you can authenticate to the local SQL Server service.

- Log on to an administrator account and check that you can perform the following tests:
  - Administer the local SQL Server service.
  - Query SQL Server tables.
  - Execute stored procedures

---

### Remote Application Interfaces

**Ensure that each application has connectivity to a back-end server or service as required.**

**Check that the system can authenticate to any required back-end servers.**

**Terminal Server**

- Attempt to initiate a Remote Desktop Protocol (RDP) session from a client computer.

- Check that you can log on as a local administrator via the RDP session.

- Test that the local administrator account can access the required admin consoles.

- Test that the RDP session is secured to the required encryption level and that server authentication succeeded.

---

Figure 31. Remote application tests
### Remote Application Interfaces

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check that you can log on as a domain administrator via the RDP session.</td>
</tr>
<tr>
<td>Test that the domain administrator account can access the required admin consoles.</td>
</tr>
<tr>
<td>Test that a standard Terminal Server user account can terminate an RDP session.</td>
</tr>
<tr>
<td>Check that a user account can recover a disconnected session.</td>
</tr>
</tbody>
</table>

#### IIS Server

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that you can authenticate to the IIS service across the network.</td>
</tr>
<tr>
<td>Authenticate as a local administrator account and check that you can administer the remote IIS service.</td>
</tr>
<tr>
<td>Check that an administrator account can retrieve both static and active (for example, ASP) pages from the remote IIS service.</td>
</tr>
<tr>
<td>Check that standard user accounts can authenticate to the remote IIS service.</td>
</tr>
<tr>
<td>Check that a standard user account can retrieve both static and active (for example, ASP) pages from the remote IIS service.</td>
</tr>
</tbody>
</table>

#### SQL Server

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check that an administrator account can log on to the SQL Server service.</td>
</tr>
<tr>
<td>Check that an administrator account can perform the following tasks:</td>
</tr>
<tr>
<td>✦ Query tables.</td>
</tr>
<tr>
<td>✦ Add and configure local (SQL Server) users.</td>
</tr>
<tr>
<td>✦ Add and configure Domain users.</td>
</tr>
<tr>
<td>✦ Execute stored procedures.</td>
</tr>
<tr>
<td>✦ Create and update tables.</td>
</tr>
<tr>
<td>✦ Remove tables.</td>
</tr>
</tbody>
</table>
Remote Application Interfaces

Check that a standard user account can perform the following tasks:

- Authenticate to the SQL Server service.
- Query tables.
- Execute stored procedures.
- Update tables.

Notes

Basic functionality tests (that is, connection, authentication, administration, and read and write functionality) apply equally to other back-end connections such as Message Queuing (also known as MSMQ), SNA Gateway, the network file system (NFS), and so on.

Testing User Applications

Figure 32 and Figure 33 list some suggested processes for testing any security updates for the Microsoft Office system and Internet Explorer. This part of the testing process requires a set of tests for all supported business applications in the organization. For Internet Explorer, IT pros should test to ensure that the page renders correctly and the application is functional before or after update installation. Again, these steps are only a baseline to start the testing process. We recommend that IT pros modify these for their organization’s specific requirements.

Figure 32. Application tests for users of the Microsoft Office system

Testing for the Microsoft Office System

Ensure that the supported service pack for the Microsoft Office system is installed on the system.

Perform typical operations in applications in the Microsoft Office system, such as opening, saving, editing, and closing files.

Verify that you can save documents, spreadsheets, and presentation files in various formats. For example, .docx, .doc, .html, .dot, and .rtf in Microsoft Office Word; .xlsx, .xls, .html, .xml, and various text formats in Microsoft Office Excel®.
## Testing for the Microsoft Office System

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run documents (including workbooks and presentations) that have macros at different security levels (low, medium, and high).</td>
<td></td>
</tr>
<tr>
<td>Run internal and other applications in the Microsoft Office system that use applications in Microsoft Visual Basic® for Applications.</td>
<td></td>
</tr>
<tr>
<td>Test that ActiveX® controls embedded in a file load without any problems, and that adding new ActiveX controls works correctly.</td>
<td></td>
</tr>
<tr>
<td>Perform the above tests with digital rights management (DRM), too. Ensure that opening, editing, and saving files with DRM works.</td>
<td></td>
</tr>
</tbody>
</table>

Figure 33. Application tests for users of Internet Explorer

## Internet Explorer Testing on Server and Workstations

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test any internally developed LOB web applications.</td>
<td></td>
</tr>
<tr>
<td>Test applicable Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) applications.</td>
<td></td>
</tr>
<tr>
<td>Test applications that use .css files, for example, Microsoft Visual Studio®.</td>
<td></td>
</tr>
<tr>
<td>Run applications that use Internet Explorer components to perform File Transfer Protocol (FTP) operations.</td>
<td></td>
</tr>
<tr>
<td>Check that web applications that use dynamic Hypertext Markup Language (DHTML) can still use:</td>
<td></td>
</tr>
<tr>
<td>✦ Pop-up objects.</td>
<td></td>
</tr>
<tr>
<td>✦ The window.location object.</td>
<td></td>
</tr>
<tr>
<td>✦ The window.opener object.</td>
<td></td>
</tr>
<tr>
<td>✦ Events.</td>
<td></td>
</tr>
<tr>
<td>✦ The &lt;object&gt; tag.</td>
<td></td>
</tr>
<tr>
<td>✦ The window.self object.</td>
<td></td>
</tr>
<tr>
<td>✦ ActiveX controls.</td>
<td></td>
</tr>
<tr>
<td>✦ Microsoft .NET controls.</td>
<td></td>
</tr>
<tr>
<td>✦ Visual Basic® Scripting Edition (VBScript) and JScript®</td>
<td></td>
</tr>
</tbody>
</table>
### Internet Explorer Testing on Server and Workstations

<table>
<thead>
<tr>
<th>Test Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check that Web applications can use cascading style sheets (CSS) and that they display correctly.</td>
</tr>
<tr>
<td>Test that Web applications using HTML pages that use binary behaviors still perform as expected.</td>
</tr>
<tr>
<td>Check that HTML pages that use external scripts still perform as expected.</td>
</tr>
<tr>
<td>Test the functionality of Web applications using HTML pages that use the <code>&lt;script&gt;</code> tag.</td>
</tr>
<tr>
<td>Test opening .mht files.</td>
</tr>
<tr>
<td>Check any application that makes use of urlmon.dll for file downloads.</td>
</tr>
<tr>
<td>Test saving Web pages.</td>
</tr>
<tr>
<td>Test HTML pages that use CSS.</td>
</tr>
<tr>
<td>Check that any applications that host Internet Explorer as a browser, such as Microsoft Office 2003 (with Web toolbar), still display pages correctly.</td>
</tr>
</tbody>
</table>

After the required update packages have passed the testing process, the next step is to pass them to the deployment mechanisms and deploy them in the organization.

### Deploying Update Packages

Within any organization, a wide variety of computer systems may require security updates. This section discusses the mechanisms that IT pros can use to help support a deployment to the vast majority of these systems with minimum disruption and effort, but still within the recommended timeframe for the deployment.

Before the package deployment starts, it is important to have an up-to-date picture of the systems that need to be updated and the systems present in the environment during the required update window. Ideally, your organization uses a monitoring and reporting solution that can create a report about the current status of all managed computer systems. This report can then be used as the basis of the deployment and passed to the Monitor Systems stage (discussed later in this guide) when deployment has started so as to track which target computers are updated and, crucially, which ones are not.

In organizations that do not use a monitoring solution that supports these reports, IT pros should find another mechanism to determine which systems need to be targeted and what their current status is.
If no other management solution is available, IT pros can scan for systems currently active on the network by using the free Microsoft Baseline Security Analyzer (MBSA) tool. MBSA is a tool that helps small- and medium-sized businesses to determine their security state in accordance with Microsoft security recommendations, and the tool also offers specific remediation guidance. Use MBSA to detect common administrative vulnerabilities and missing security updates on computer systems. See technet.microsoft.com/security/cc184924.aspx.

The MBSA tool does not install updates; it can only scan for updates and configure the computer to use Microsoft Update for update management. The MBSA tool is not a replacement for a full systems management inventory tool, but it can be used for environments where no inventory solution is in place.

Larger Enterprise organizations will likely require additional capabilities that MBSA does not provide. System Center Configuration Manager is another solution that provides additional features that MBSA and WSUS do not provide. See www.microsoft.com/systemcenter/configurationmanager/.

Several potential issues and constraints may dictate the steps that are necessary to fully deploy the security update into production. When IT pros are tasked with deploying a security update, they should consider the information in Figure 34.

Figure 34. Package deployment considerations

<table>
<thead>
<tr>
<th>Deployment considerations</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consider how to handle the exceptions to the timeline requirements.</td>
<td>The amount of time that the target systems have before they need to be updated should be dictated as part of the Risk Evaluation process. However, some systems may not meet these timelines. Therefore, it is important that IT pros have a documented process to follow so that these systems do not fail to receive updates. Several factors can lead to this situation including system availability, user roles and responsibilities, and the nature of the system instability or security vulnerability that the update is designed to address.</td>
</tr>
<tr>
<td>Deployment considerations</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ensure that systems meet the minimum installation requirements.</td>
<td>If the update requires a certain amount of disk space to install, or you want to cache the update locally before installation, you must instigate a check on the amount of free disk space on each client computer in the organization. In addition, remote client computers may take some time to download large updates. If the update is not classified as mandatory, it may be appropriate to postpone installation on remote client computers until they are physically connected to the network. However, after the update becomes mandatory, all client computers should be forced to apply updates, including client computers that are remote.</td>
</tr>
<tr>
<td>Plan for update timeframes and time zones.</td>
<td>Business-critical computers may have specific times at which changes and computer restarts are permitted (outage windows). You must schedule the deployment of a security update and any system restarts that are required as a result within these outage windows. It can also be beneficial to stage the update so that clients are updated at different times. Sometimes, using time zones can help to manage these deployments. IT pros using WSUS can use Group Policy settings to force client computers to install an update before a regularly scheduled maintenance window. However, before doing this, make sure that there is a forced replication on any child WSUS servers. These are normally scheduled to synchronize updates at quiet times on the network, using the Synchronize Now option on the WSUS Server Administration Page. See the Deploying Microsoft Windows Server Update Services guide for more information: technet.microsoft.com/library/cc720507(WS.10).aspx.</td>
</tr>
<tr>
<td>What is the status of any Group Policy restrictions?</td>
<td>If client computers are locked down through the use of certain Group Policy settings, this may affect the ability of security updates to install correctly.</td>
</tr>
<tr>
<td>Determine whether any of the updates require access to original installation files.</td>
<td>If the product to be updated was deployed by using Windows Installer, Windows Installer may require access to original installation files. If an unattended installation of the security update is performed, these files need to be in the same location as they were when the product was originally installed. If the product was originally installed from physical media—a CD drive, for example—Windows Installer will try to find the original files on the currently inserted CD.</td>
</tr>
<tr>
<td>Deployment considerations</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Check to see whether any user applications were installed on a per-user basis.</td>
<td>If any applications were installed on a per-user basis, rather than on a per-computer basis for all users, IT pros should reinstall the application on a per-computer basis and then apply the security update to the new installation.</td>
</tr>
<tr>
<td>Plan for network bandwidth constraints.</td>
<td>There may be compelling reasons to apply the security update to computers that are at risk from a security vulnerability or potential system instability and then, after these computers are updated, continue the rollout elsewhere. For example, deploying security updates to remote sites is likely to take longer than for local sites because of network bandwidth constraints. In these cases, it might be optimal to consider deploying locally first to get the maximum number of systems updated in the shortest time period. You can deploy the security update at the remote sites after the local deployment time window has completed.</td>
</tr>
</tbody>
</table>

Some of these considerations may require IT pros to make modifications to the original deployment plan. If this is the case, it is important to check the SLAs. If the deployment cannot meet the SLA requirements, this should be communicated to the appropriate individuals so they can evaluate the risk that it poses to the organization.

**Submitting a Change Request**

The next step is for IT pros to submit a change request for the production systems that are managed through a standard change control process. After IT pros have submitted the necessary change requests, they must determine how and when information about the security update—such as its severity, impact, and the steps that need to be taken to deploy it—will be communicated to users, the business, and the service desk.

This should be included in the deployment plan that is mentioned above.

**Communicating the Rollout Schedule to the Organization**

It is important to tell end users and administrators about the impending release of an update. IT pros should send a clear and easily identifiable email message to users and administrators, which both notifies them of the update and provides information about how to install it. If possible, IT pros should flag the email message for follow-up to remind users and administrators of the actions that they need to take.

*Common intranet home page.* If your organization has a common intranet
home page for users, consider posting a notice on this site for the duration of the update timeline.

**Wake-on-LAN functionality.** If your organization is deploying an update to desktop computers outside core business hours, create a notice to tell users to leave their computers on overnight on a specified date unless the organization has Wake-on-LAN functionality enabled on those systems.

**Using WSUS policy options.** Using WSUS, IT pros also have the option to notify the users directly by using the update notifications. These are pop-up messages that are delivered directly to the user’s system when the deployment package is ready. If this is the case, IT pros may need to consider some additional options as to how they offer this package. Figure 35 discusses these options.

For more detailed information about using WSUS in the deployment phase, see the Windows Server Update Services (WSUS) TechNet Library at technet.microsoft.com/library/cc706995(WS.10).aspx.

**Installing the Update**

When a release plan is in place and has been communicated, the next stage of the deployment process is to install the required update on systems. The tasks and activities that you need to perform here primarily depend on the requirements of
the organization's deployment mechanism. This step may require various mechanisms to reach all of the systems. For example, it is possible to use the Standard Update Deployment Timeline process for client systems. However, for Hyper-V™ servers, the systems administrators are likely to conduct the update manually so that they can watch it closely and get the server back to a fully operational state as quickly as possible.

Larger organizations are likely to have an additional layer of complexity that requires IT pros to balance the update workload across several update servers and stage the updates on those servers in the organization to help ensure that the number of client updates does not overload any one server. Ideally, IT pros should release security updates through a phased deployment, as was discussed earlier in this stage. This minimizes the impact of any failures or adverse effects that might occur during the initial distribution of a security update.

The steps of this process are dependent on the infrastructure management products that IT pros use to deploy the update. However, tools aside, certain stages are typically required, which include:

- **Staging the required updates on the deployment servers.** Copy the required updates to the deployment servers ready to advertise them to the update clients.

- **Distributing the update package to the required clients.** How IT pros manage this stage depends heavily on the number of clients that are included in the update process and the capabilities of the organization's update service. If IT pros support a large number of clients, the distribution process is likely to involve either staging the update package across several servers to help spread the workload, or performing a rolling update where the client base is updated over a period of time so that an acceptable maximum limit is maintained on the update server.

- **Executing the update package.** Again, how the package is executed will depend on the management tools, but IT pros have two basic options: Automated or Manual.

**Approving the update on WSUS.** If a phased rollout is not required, IT pros only need to approve the update on the WSUS parent server for it to be made available to clients. WSUS clients will then begin to download the newly approved update, either at the next detection cycle or when prompted by the local administrator (if the Automatic Updates client has been configured to notify the local administrator when new updates are available).

However, if there is to be a phased rollout, IT pros should first approve the update on the parent WSUS server only. Then, after they have successfully deployed the update to client computers that are supported by that server, they should enable synchronization of the approvals list on the WSUS child server that supports client computers in the next phase of the rollout.
Accelerating Security Update Deployment

If the security update was prioritized as an urgent update, the package application process must typically be accelerated to ensure that the update is deployed within the shortest possible time period. Security update deployment can be accelerated using one of two methods:

1. Use the same basic process as for the standard update timeline, but with additional workforce to speed up the process.
2. Use a simpler process that minimizes the effort that is required to send out the update.

With either approach, the goal is to minimize the time that the “unpatched” systems remain able to connect to the organization’s networks. This means that it is imperative for IT pros to have the necessary records to identify and validate the devices that require an update against those that have already received the updates. The ability to do this in an automated and reliable manner is helpful for all update deployments, but crucial for urgent ones.

Creating Update Packages

The process for creating packages remains basically the same for both ordinary and expedited deployments. However, if an update is identified as likely to be high risk as part of the evaluation, it is important to give the deployment team as much notice as possible to prepare for the update.

Testing Packages

The full testing process for an update requires a significant investment to ensure that all supported system configurations are tested. For some organizations, this full testing cycle presents an unacceptable delay in the update deployment process. In these cases, a limited field-testing option may help to provide a faster deployment process. For example, some organizations will test an urgent update directly on a select group of production systems as a beta test environment rather than using a lab environment. As long as this initial installation is successful, the full deployment will be mandated and possibly even automated to occur as soon as an out-of-date system attempts to connect back to the organization’s network.

For server updates, this process could start on non-production servers and only roll out to the production servers after the updates have been validated on these lower-priority servers.

Deploying Packages

For urgent deployments, the time between the update first being offered and the time when the update switches from optional to mandatory is likely to be much shorter than for normal deployments. Instead of having days or even weeks to apply the update, it is more likely that the system’s users and administrators will have only a matter of hours before the update is required. This will likely lead to
a situation where systems are not online during this period of time, and they will therefore have to be updated as soon as they are next connected.

To handle this situation, it is important that IT pros monitor the deployment process and track the status of the clients that still require the update. This is the focus of the final stage in the customer risk-management framework.

**Stage 5: Monitor Systems**

**This section covers:**
- Confirming successful update deployment.
- Uninstalling a security update.
- Post-implementation review.
- A reminder about short-term mitigation removal.

**At the end of this section, IT pros should:**
- Understand methods to confirm or deny successful update installation:
  - Using scripts.
  - Using the Microsoft Baseline Security Analyzer (MBSA) tool.
  - Using file version verification.
  - System Center Configuration Manager.
  - Other installation and security update detection tools.
- Understand the resources and methods for uninstalling a security update.
- Understand the general steps for a post-implementation review.

**Microsoft resources referenced in this section:**
- **Microsoft Script Center.** See [www.microsoft.com/technet/scriptcenter](http://www.microsoft.com/technet/scriptcenter).
- **Microsoft Baseline Security Analyzer (MBSA)**. This is a tool that helps small and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. The MBSA tool can help detect common administrative vulnerabilities and missing security updates on computer systems. MBSA does not perform the installation of updates; the tool only scans for updates and has the ability to configure the computer to use...

- **System Center Configuration Manager.** See www.microsoft.com/systemcenter/configurationmanager/.

- **Microsoft Customer Service & Support (CSS).** Contact CSS either through your organization’s existing Microsoft support contacts or by calling (1) (866) PC-SAFETY [(1) (866) 727-2338 in the United States and Canada.] Internationally, IT pros should contact their local Microsoft subsidiary. See support.microsoft.com/common/international.aspx.

The Monitor Systems stage helps to ensure that the current security updates are deployed successfully and that future update cycles continue to run smoothly. Figure 36 shows a summary of the steps required during this stage.

**Successful Update Deployment**

The first task during the Monitor Systems stage is to quickly determine which systems successfully deployed the update and which systems did not. The update installation can fail for several reasons, including but not limited to the reasons in the following list:

- The computer is offline.
- The computer is being rebuilt or reimaged.
- The computer has insufficient disk space.
- The computer is not communicating with the update server.
- The required update client software is not running on the computer.
- The computer is missing some dependent software.

Whatever the reason, it is at this point that the deployment support teams are likely to be required to help troubleshoot the remaining systems. If this process takes the systems outside their update window, it is important to inform the
appropriate administrators so that they can determine the risk that this situation poses to the organization. For high risk situations, this may involve removing the systems that have not successfully applied the updates from the organization’s network until they can be manually updated offline.

**Confirming Update Installation**

Several mechanisms to confirm whether the update was successfully installed on systems can be used. These include:

- **Computer management reporting.** If the computer management system supports the ability to report on security update versions, this option is typically the quickest and easiest method of confirming the installation of the update.

- **Remote script queries.** Depending on the variety of operating systems in the organization, IT pros may be able to use a scripting environment such as Windows Script Host (WSH) or Windows PowerShell™ to query the computers for their status. For this method to be successful, it is important that all the systems to be checked support both the scripting environment and the ability to query remotely.

For more information about WSH and Windows PowerShell, see the Microsoft Script Center at [www.microsoft.com/technet/scriptcenter](http://www.microsoft.com/technet/scriptcenter).


- **Microsoft Baseline Security Analyzer (MBSA)**\(^\text{11}\). This tool provides another excellent method to confirm whether a security update was successfully installed. It is possible to configure this tool to remotely query a computer to determine its security update status.

To download the latest version of the MBSA tool and for more information, see [technet.microsoft.com/security/cc184923.aspx](http://technet.microsoft.com/security/cc184923.aspx).

The MBSA tool provides support for performing the security update portion of a scan against the Update Services server to which each scanned computer is assigned. In addition, it performs a stand-alone scan for organizations that do not have an Update Services server. Administrators can select options in the MBSA tool to ignore or exclusively observe the approved list of updates on the Update Services server. However, by default, the security scan occurs against the list of approved security updates on the Update Services server and against the complete list of available security updates available in the Microsoft Update catalog. Items not approved on the Update Services server for the scanned computer are given an informational score only and do not count against the

---

\(^\text{11}\) MBSA is localized into four languages (English, German, French, and Japanese), but the underlying detection accurately scans target computers in any language that Microsoft Update and WSUS support.
cumulative security assessment score. Items that are approved, but are not installed on the target computer, are given an appropriate warning and are considered security risks. The MBSA tool provides an Advanced Update Services option to enable target computers that do not have an assigned Update Services server to report an error so that the help desk can clearly identify them. At a command prompt, this is provided by the \wa (WSUS approved) option.

Other installation and detection tools. There are several other security update deployment and detection tools that can also be used to confirm that a system has been updated. We recommend that IT pros use tools that confirm security update installation rather than those that perform specific vulnerability testing.

File version verification. If the MBSA tool or another tool is not an option for IT pros, Microsoft also provides information for the respective package in the Knowledge Base article and security bulletin in the “File Version Verification” section. There are several versions and editions of Windows, so the following steps may be different. If so, consult the product documentation to complete these steps. However, generally, file version verification follows these steps:

1. Click Start (in Windows Vista and Windows 7, Start is represented by the icon below), click Start Search, and then type an update file name.

2. Under Programs, right-click the file name, and then click Properties.

3. On the General tab, compare the file size with the file information tables that are provided in the security bulletin Knowledge Base article.

4. You may also click the Details tab and compare information, such as file version and date modified, with the file information tables that are provided in the security bulletin Knowledge Base article.

5. Finally, you may click the Previous Versions tab and compare file information for the previous version of the file with the file information for the new, or updated, version of the file.

Some applications do not have any supported tools. Therefore, file version verification is the only method to confirm successful installation.

System Center Configuration Manager. As previously mentioned, larger Enterprise organizations will likely require additional capabilities that the MBSA tool does not provide. Therefore, Microsoft System Center Configuration Manager is another solution that provides additional features that the MBSA tool and WSUS do not provide. See www.microsoft.com/systemcenter/configurationmanager/.
Even after a system has successfully completed an update, we recommend to allocate time to monitor for any unidentified post-update issues that might cause either loss of functionality or performance degradation.

Although it is rare for issues like this to appear after a successful set of acceptance tests, it is possible, especially on client computers that may be running nonstandard system configurations or applications.

**Uninstalling Security Updates**

Most, though not all, Microsoft security updates can be uninstalled, and there may be times when IT pros need to rapidly uninstall a security update. Obviously, uninstalling a security update can leave the system and network vulnerable. In addition, if the security update for the affected software is not installed, it will continue to appear as an update on Microsoft Update. Nevertheless, Figure 37 through Figure 39 provide quick-reference instructions for how to uninstall a security update on various products.

**Figure 37. Instructions for removing an update from the operating system**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the Add or Remove Programs folder in Control Panel or the Spuninst.exe utility that is located in the %Windir%$NTUninstallKB[XXXXXX]$\Spuninst folder.</td>
<td>Wusa.exe does not support uninstalling updates. To uninstall an update that Wusa.exe has provided, click Control Panel, and then click Security. Under Windows Update, click View installed updates, and then select the update that needs to be removed from the list that appears.</td>
</tr>
</tbody>
</table>

**Figure 38. Instructions for removing an update from the Microsoft Office system**

<table>
<thead>
<tr>
<th>Microsoft Office XP and Microsoft Office 2003 (all editions)</th>
<th>Microsoft Office 2007 and Microsoft Office 2010 (all editions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Office XP and Microsoft Office 2003 (all editions)</td>
<td>Microsoft Office 2007 and Microsoft Office 2010 (all editions)</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Use the Add or Remove Programs folder in Control Panel.</td>
<td>Use the Add or Remove Programs folder in Control Panel.</td>
</tr>
</tbody>
</table>

**Note:** When removing this update, you may be prompted to insert the Microsoft Office XP CD. In addition, you may not have the option to uninstall the update from the Add or Remove Programs folder in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 828451 ([support.microsoft.com/kb/828451](support.microsoft.com/kb/828451)).

Figure 39. Instructions for removing an update from Internet Explorer

<table>
<thead>
<tr>
<th>Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8 on Windows XP and Windows Server 2003</th>
<th>Internet Explorer in Windows Vista, Windows 7, and Windows Server 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Internet Explorer 6, use the Add or Remove Programs folder in Control Panel or the Spuninst.exe utility that is located in the %Windir%$NTUninstallKB[XXXXXX]$\Spuninst folder.</td>
<td>Wusa.exe does not support uninstalling updates. To uninstall an update that Wusa.exe has installed, click Control Panel, and then click Security. Under Windows Update, click View installed updates, and then select from the list of updates.</td>
</tr>
<tr>
<td>For Internet Explorer® 7, use the Add or Remove Programs folder in Control Panel or the Spuninst.exe utility that is located in the %Windir%\ie7updates\KB[XXXXXX]-IE7\spuninst folder.</td>
<td>For more information about Wusa.exe, see <a href="support.microsoft.com/kb/934307">support.microsoft.com/kb/934307</a>.</td>
</tr>
<tr>
<td>For Internet Explorer® 8, Use Add or Remove Programs folder in Control Panel or the Spuninst.exe utility located in the %Windir%\ie8updates\KB[XXXXXX]-IE8\spuninst folder</td>
<td></td>
</tr>
</tbody>
</table>

If IT pros have referenced the security bulletin and associated Knowledge Base
article, but still cannot uninstall the security update, they should contact CSS either through their organization’s existing Microsoft support contacts or by calling (1) (866) PC-SAFETY [(1) (866) 727-2338 in the United States and Canada.] Internationally, IT pros should contact their local Microsoft subsidiary. See support.microsoft.com/common/international.aspx.

The team will be able to gather case-specific information to help assess the issue and assist in identifying a resolution.

**Post-Implementation Review**

The post-implementation review should typically be conducted within one to four weeks of a release deployment to identify improvements that should be made to the update management process. Usually, key members of the security update deployment and support teams conduct this review. Recommended agenda topics for a review include:

- Ensure that the vulnerabilities are added to vulnerability scanning reports and security policy standards.
- Ensure that build images and any offline virtual machine drive files have been updated to include the latest security updates following the deployment.
- Discuss planned results versus actual results.
- Discuss the risks associated with the release.
- Review the organization’s performance throughout the incident. Take this opportunity to improve the organization’s response plan to include any lessons learned.
- Discuss changes to any service windows.
- Determine whether the update system is still meeting the requirements of the organization.
- Assess any incident damage and costs, including both downtime and recovery costs.
- Create another baseline or update the existing baseline for your environment.

The overall goal of this meeting is to ensure that any lessons learned during the update process are communicated and incorporated into future update cycles.

**Short-Term Mitigation Removal**

The final step before the whole process resets to await the next release is the removal of any short-term mitigation that is no longer required. Typically, a short-term mitigation will have some impact on the normal operations of the organization. While the organization’s systems were at risk, this impact was acceptable. However, after the updates are successfully in place, it is necessary to remove the mitigations to return the organization to normal operations.
Stage 6: Use Microsoft Resources to Track Security Developments

This section covers:

- Major and minor revisions to Microsoft security bulletins and advisories.
- Microsoft resources to help combat the threat of malicious software (malware).

At the end of this section, IT pros should:

- Understand major and minor security bulletin and advisory revisions:
  - What these mean.
  - How IT pros can stay informed of any revisions.
  - Where to look on security bulletins and advisories for any revisions.
- The Microsoft Malware Protection Center (MMPC) is the authoritative, global voice from Microsoft on anti-malware research, protection, and guidance on the Windows platform. The MMPC has many resources and solutions that include:
  - The Microsoft Security Intelligence Report.
  - The Microsoft Malware Protection Center Blog and Security Portal.
  - The Microsoft Windows Malicious Software Removal Tool.
  - Windows Defender.
- Other Microsoft security resources.

Microsoft resources referenced in this section:

- **Microsoft Security Intelligence Report.** A semi-annual report that uses data derived from hundreds of millions of Windows users to provide an in-depth perspective on the changing threat landscape, including software vulnerability disclosures and exploits, malicious software, and potentially unwanted software, and more. See [www.microsoft.com/sir](http://www.microsoft.com/sir).

- **Microsoft Malware Protection Center (MMPC) Security Portal.** This website contains details about top threats, a malicious software encyclopedia, malicious software tools and resources, and a malicious software sample submission mechanism. See [www.microsoft.com/security/portal/](http://www.microsoft.com/security/portal/).

- **Microsoft Malware Protection Center (MMPC) Blog.** This blog includes real-time communication from MMPC subject-matter experts on topics covering new, emerging, and notable malicious software threats and other research topics in the computer security field. See [blogs.technet.com/mmpc/](http://blogs.technet.com/mmpc/).

- **The Microsoft Windows Malicious Software Removal Tool (MSRT).** The
MSRT checks computers running supported Windows operating systems for infections by specific, prevalent, malicious software, and helps remove any infection found. See www.microsoft.com/security/malwareremove/.

- **Windows Defender.** This software helps protect computers against pop-up windows, slow performance, and security threats that spyware and other potentially unwanted software can cause. See www.microsoft.com/windows/products/winfamily/defender.

- **Trustworthy Computing (TwC) Security and Privacy Blog Aggregator.** This page dynamically consolidates and features security and privacy blogs. See www.microsoft.com/twc/blogs.

- **Security Solution Accelerators.** A free collection of tools and guidance to help IT pros proactively plan, integrate, and operate their security infrastructure. See www.microsoft.com/ssa.

- **Security Risk Management Guide.** A technology-agnostic solution that provides a four-phased approach to risk-management. The guide references many industry-accepted standards for managing security risk and incorporates real-world experiences from Microsoft IT and partners. See go.microsoft.com/fwlink/?linkid=30794.

- **IT Infrastructure Threat Modeling Guide.** A method for developing threat models that helps prioritize investments in IT infrastructure security. This guide describes and considers the extensive methodology that exists for SDL threat modeling and uses it to establish a threat-modeling process for the IT infrastructure. See go.microsoft.com/fwlink/?LinkId=154010.

Unfortunately, successful deployment of security updates does not end security management duties. In today’s evolving threat landscape, it is imperative to always remain alert. As discussed in “Stage 1: Receive Microsoft Security Release Communications” earlier in this guide, Microsoft Technical Security notifications and MSRC blog alerts provide updates on any news or communications from Microsoft that relates to your organization’s security posture.

**Major and Minor Security Bulletin and Advisory Revisions**

Providing you are signed up to receive Microsoft security notifications, you may receive email messages from Microsoft notifying you of a security bulletin or security advisory revision after its original release. There are two types of revisions: minor and major.

Major revisions are more notable and can affect the release binary, which typically requires IT pros to reinstall a security update. Major revisions often result from a product being added to or subtracted from the affected or non-affected software section of the security bulletin; or if the severity rating is revised for a particular product. Therefore, if a notice for a major bulletin or advisory
revision is received, it is important to carefully read the notice and take the necessary actions.

Minor revisions mostly result from a change in the security bulletin's textual context and therefore do not hamper an organization's security; but IT pros should still make note of the revision. In addition, Microsoft does not notify IT pros of revisions that do not affect facts or correct spelling errors.

Another way to check for security bulletin and security advisory revisions is in the documents themselves. Revisions are noted in two places:

1. The bulletin or advisory header (see Figure 40).

Figure 40. Security bulletin header

![Microsoft Security Bulletin MS09-014 - Critical Cumulative Security Update for Internet Explorer (963027)](image)

Version: 1.2

Published: April 14, 2009 | Updated: April 22, 2009

2. The bulletin footer, which details the revision history (see Figure 41).

Figure 41. Security bulletin footer

![Revisions](image)

- **V2.0** (April 29, 2009): Added Microsoft XML Core Services 4.0 (KB954430) on 32-bit and x64-based editions of Windows Vista Service Pack 2 and on 32-bit, x64-based, and Itanium-based editions of Windows Server 2008 Service Pack 2 as affected software. Also added as non-affected software: Microsoft XML Core Services 3.0 and Microsoft XML Core Services 6.0 on 32-bit and x64-based editions of Windows Vista Service Pack 2 and on 32-bit, x64-based, and Itanium-based editions of Windows Server 2008 Service Pack 2. This is a detection change only; there were no changes to the binaries. Customers who have already successfully installed KB954430 do not need to reinstall.

All security bulletins and advisories are initially released as 1.0. A minor revision has an X.1 increase and a major revision has a 1.X increase. Therefore, a security bulletin or advisory that is labeled as 2.3 has undergone one major revision and three minor revisions.

**The Constant Threat from Malicious Software**

Malicious and potentially unwanted software is increasingly becoming a global phenomenon because criminals are creating software targeting users and
computers in many languages and many different countries. These threats continue to exploit human nature and software applications far more than vulnerabilities in web browsers or operating systems. As Microsoft has moved forward with securing its operating systems and applications via the Security Development Lifecycle (SDL), in an effort to get their software onto victims’ computers, criminals are shifting their focus to other applications, browser add-ons, and direct appeals to human emotion.

A particularly prominent way in which criminals are taking advantage of this trend is by persuading users to download and install fake antivirus or antispyware software that may be malicious in nature. After criminals have tricked a victim into installing this rogue security software, they may have obtained the victim’s credit card details or established a pathway for downloading more malicious software onto the infected computer. Microsoft security products and services removed rogue security software from more than 10 million computers worldwide during the first half of 2010 and will continue to target these threats in the future.

The Microsoft Malware Protection Center (MMPC) is the authoritative global voice of anti-malware research, protection, and guidance on the Windows platform. Among other things, this group is a leading contributor to the Microsoft Security Intelligence Report (SIR) (See www.microsoft.com/sir), which provides an in-depth perspective on the changing threat landscape. The SIR includes detailed analysis of software vulnerability disclosures and exploit trends; security and privacy breaches; malicious software and potentially unwanted software; and email, spam, and phishing trends. Each report focuses on data and trends that were observed in the first or second half of each calendar year and uses historical data to provide context. The purpose of the SIR is to keep IT pros informed of the major trends in the threat landscape and provide valuable insights and security guidance that help IT pros improve their security posture in the face of these threats.

During your organization’s normal operations, you should take steps to ensure you are kept up to date on any new malicious software that exploits vulnerabilities. If assistance is required, see the following helpful malicious software resources:

- **MMPC security portal.** This is a comprehensive website that contains details of top threats, an in-depth malicious software encyclopedia, malicious software tools and resources, and a malicious software sample submission mechanism. See www.microsoft.com/security/portal.

- **MMPC blog.** This provides a real-time method for MMPC subject-matter experts to communicate with customers. Topics include “behind the scenes” information about new, emerging, and notable malicious software threats; in addition to other research topics in the computer security field. See blogs.technet.com/mmpc/.

- **The Microsoft Windows Malicious Software Removal Tool (MSRT).** This is a free tool to help identify and remove prevalent malicious software.
families from customer computers. The MSRT is released as an Important update through Windows Update and Microsoft Update. A version of the tool is also available from the Microsoft Download Center. The MSRT helps remove specific, prevalent malicious software from computers running Windows 7, Windows Vista, Windows XP, Windows Server 2008, Windows Server 2003, and Windows 2000. As of February 2011, the tool detects and removes 155 malicious software families; most of which are currently prevalent or were prevalent at the time that they were added. When the detection and removal process is complete, the tool displays a report that describes the outcome, including which, if any, malicious software was detected and removed. See www.microsoft.com/security/malwareremove/.

**Note:** The MSRT is not a replacement for an up to date antivirus solution because it lacks real-time protection and uses only the portion of the Microsoft antivirus signature database that enables it to target specifically selected, prevalent malicious software.

- **Windows Defender.** This software helps protect your computer against pop-up windows, slow performance, and security threats that spyware and other unwanted software can cause. It does so by detecting and removing known spyware from your computer. Windows Defender features Real-Time Protection – a monitoring system that recommends actions against spyware when it is detected, minimizes interruptions, and helps users to stay productive. See www.microsoft.com/windows/products/winfamily/defender.

**Other Security Resources**

**Microsoft Trustworthy Computing (TwC) Group Security and Privacy Blog Aggregator.** This page dynamically consolidates and features blogs from Microsoft Trustworthy Computing (TwC): the team charged with working to deliver more secure, private and reliable computing experiences. Read about the long-term vision and strategy from Microsoft for computing privacy and security.

You can access the Trustworthy Computing Security and Privacy blog aggregator at www.microsoft.com/twc/blogs.

**Security Solution Accelerators** are a collection of tools and guidance. They are free, authoritative resources to help IT pros to proactively plan, integrate, and operate their security infrastructure. See www.microsoft.com/ssa.

The **Security Risk Management Guide** is a technology-agnostic solution that provides a four-phased approach to risk-management. The guide references many industry-accepted standards for managing security risk, incorporates real-world experiences from Microsoft IT, and also includes input from Microsoft IT pros and partners. See go.microsoft.com/fwlink/?linkid=30794.

The **IT Infrastructure Threat Modeling Guide** provides an easy-to-understand method for developing threat models that can help to prioritize investments in IT infrastructure security. It describes and considers the extensive methodology that exists for SDL threat modeling and uses it to establish a threat-modeling process
for the IT infrastructure. See go.microsoft.com/fwlink/?LinkId=154010.

Summary

The security update deployment process has become a necessary part of the systems management routine for any Internet-connected environment. Criminals are now targeting their malicious software at operating systems and applications from various vendors, not just Microsoft. Therefore, a failure to keep your organization's systems and applications updated can put users at serious risk of attack from criminals and the malicious software they develop.

The complete Microsoft Security Update Release and Deployment process diagram is in the Appendix of this guide.

Microsoft is committed to providing an effective and timely response to any vulnerability in its software. It is working with many industry partners to ensure that customers receive industry-leading levels of protection to counter the criminals who attempt to attack your computers.

The information that Microsoft provides in this guide is designed to support your risk management decisions. This guide is designed to help IT pros understand, utilize, and maximize all attendant Microsoft communications, guidance, programs, and services that help deploy the security updates across the organization quickly, and with a minimum amount of disruption to productivity.

For the very latest information about this and other security-related topics, see www.microsoft.com/security/msrc or www.microsoft.com/technet/security.

Feedback

Thank you for reading this guide. The authors of this guide are interested in feedback and thoughts on how your needs can be better addressed. Please feel free to share any feedback or thoughts on how you feel that Microsoft can help improve this content.

Please send your feedback to the Trustworthy Computing Security Update Guide team at twcseclb@microsoft.com.
Appendix

The Microsoft Security Update Release and Deployment Process Diagram
Microsoft Security Update Terminology

This section covers:

- Microsoft software update terminology.
- Managing non-security, or system software updates.
- The advantages of Windows Update versus Microsoft Update.
- The security update policy for non-genuine Microsoft software.

At the end of this section, IT pros should:

- Understand the different types of Microsoft software updates.
- Understand the differences between Windows Update and Microsoft Update, and the resources for how to configure each of them.
- Understand the Microsoft security update policy for non-genuine Microsoft software.

Microsoft resources referenced in this section:

- **Managing system software updates.** For information about managing the software updates that IT pros need to deploy to servers, desktop computers, and mobile computers in the organization, see technet.microsoft.com/updatemanagement/.

- **Windows Server Update Services (WSUS) and Updates.** This page helps explain how WSUS stores and manages Microsoft updates. See technet.microsoft.com/en-us/updatemanagement/default.aspx.

- **The Microsoft Windows Malicious Software Removal Tool (MSRT).** The MSRT checks computers running supported Windows operating systems for infections by specific, prevalent, malicious software, and helps remove any infection found. See www.microsoft.com/security/malwareremove/.

- **Microsoft Download Center.** See www.microsoft.com/download.

- **Windows Update.** This free, built-in service helps to keep computers more secure and reliable, and also compatible with devices. Windows Update provides new features that may enhance the Windows experience. See www.microsoft.com/windows/downloads/windowsupdate/.

- **Microsoft Update.** This free, built-in service is included with Windows. It provides a single location for getting updates and scheduling automatic updating. In addition, customers can get security and non-security updates for Microsoft software, such as the Microsoft Office system and the Windows Live® network of Internet services. See update.microsoft.com/microsoftupdate.

- **Microsoft Update Solution Center.** This contains help and support, including solutions for the most common issues with using Windows Update and explanations of error messages. See
Microsoft Security Updates

Microsoft and the MSRC often address vulnerabilities in products by releasing security updates that replace the vulnerable code with new code that has been developed and tested to address the vulnerability. Creating a security update is an extensive process, involving a series of sequential steps. Many factors affect the length of time between the discovery of a vulnerability and the release of a security update, and every vulnerability presents its own unique challenges. However, in general, when a potential vulnerability is reported to Microsoft, a designated security engineer investigates the scope and impact of a threat on the affected product. When the MSRC knows the extent and severity of the vulnerability, it works with the appropriate Microsoft product team to develop a security update for every supported version of the product that is affected. Finally, after this team has built the security update, it must be tested using numerous combinations and permutations of the various supported operating systems, applications, and even languages that it affects across the globe.

Security updates are not appropriate for every situation, so Microsoft also releases security advisories—communications from Microsoft about information that is material to an organization’s security. See page 21 for more information about security advisories and how they differ from security updates.

Security Updates and Software Updates

Microsoft makes a clear distinction between security updates and ordinary software updates. Microsoft software updates include many different kinds of changes and additions to the operating system, programs, and other software, such as a newer version of a device driver or an improvement for an application. A Microsoft security update is a software update that addresses a security vulnerability reported by a security researcher. This guide focuses solely on Microsoft security updates. Visit technet.microsoft.com/updatemanagement for general information about software updates and maintaining Microsoft systems.

The following are some of the update classifications used by Microsoft update services, including Windows Update, Microsoft Update, and Windows Server Update Services (WSUS):

- **Security updates**: A broadly released fix for a product-specific security-related vulnerability. Security vulnerabilities are rated based on their severity, which is assigned by the MSRC and indicated in the Microsoft security bulletin as critical, important, moderate, or low (severity ratings are discussed in more detail later).

- **Critical updates**: A broadly released fix for a specific problem addressing a critical, non-security or security related bug. An example of a critical update is an update for the Microsoft Windows Malicious Software Removal Tool (MSRT). Update classifications can overlap—many security updates are also critical updates.
Definition updates: A broadly released and frequent software update containing additions to a product’s definition database. Definition databases are used by security products, such as Microsoft Security Essentials and the Microsoft Forefront line of products. They are often used to detect objects with specific attributes, such as malicious code, phishing websites, or junk mail.

Update Rollups: A tested, cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a component of a product. Among others, one example of an update rollup is a service pack.

Service Packs: A tested, cumulative set of hotfixes, security updates, critical updates, and updates, as well as additional fixes for problems found internally since the release of the product. Service Packs might also contain a limited number of customer-requested design changes or features.

Feature packs: New product functionality usually included in the next full product release. Feature packs may include new security features and improvements.

Hotfixes: A hotfix is code that fixes a bug in a product. Hotfixes are sometimes packaged as a set of fixes called a combined hotfix or a service pack.

Regardless of classification, from the client-side operating system perspective, all Microsoft update are designated as either Important, Recommended, or Optional:

Important (or High Priority in Windows XP) updates offer significant benefits, such as improved security, privacy, and reliability. Important updates should be installed as they become available.

Recommended (or Optional in Windows XP) updates address non-critical problems or enhance customer computing experiences. While these updates do not address fundamental issues with the system, they can offer meaningful improvements, such as improved application compatibility, feature improvements, and more.

Optional updates can include updates, drivers, or new applications from Microsoft or its partners to enhance customer computing experiences. These updates need to be installed manually; that is, optional updates are not downloaded or installed automatically, but Windows Update provides them for review.

Downloading and installing the latest software updates, particularly Important and Recommended updates, quickly and consistently on your computer is vital to help maintain its security and proper functioning. For IT pros, applying updates on computers across the organization, whatever its size, is crucial for helping to keep systems secure and running properly.

Security updates can be downloaded individually from the Microsoft Download Center (www.microsoft.com/download). However, many IT departments use a Microsoft update service or product to automate update deployments across an
organization.

Windows Update—a free, built-in service included with Microsoft Windows—helps organizations keep computers more secure and reliable, and also compatible with devices and applications. It provides a single location to retrieve updates and scheduling automatic updating.

The Windows Update client (and the Automatic Updates client in Windows XP) will, by default, only check for Windows updates. To get updates for Windows and other Microsoft software, IT pros should configure Windows Update to check for updates using the Microsoft Update service. Microsoft Update is recommended for all computers running the Windows operating system to ensure that you are informed about any available security and software updates from Microsoft. To use Microsoft Update, see update.microsoft.com/microsoftupdate.

Windows Update has slightly different settings in the Windows Vista®, Windows 7, and Windows XP operating systems. For more information about Windows Update and its features, see www.microsoft.com/windows/downloads/windowsupdate/.

---

**Windows Update or Microsoft Update?**

Configure the computer to use Microsoft Update instead of Office Update or Windows Update. This will help to ensure that the computer receives security updates for the Microsoft Office system and other Microsoft applications, in addition to security updates for Windows operating systems. For an explanation of the differences between Microsoft Update and Windows Update, see www.microsoft.com/windows/downloads/windowsupdate/microsoftupdate.mspx.

For additional information about the Windows Update process, see the white paper called “Windows Update Explained,” available at download.microsoft.com/download/a/9/4/a94af289-a798-4143-a3f8-77004f7c2fd3/Windows%20Update%20Explained.docx. For support and troubleshooting information regarding technical problems with Microsoft Update, see support.microsoft.com/ph/6527#tab3.

For help and support, including solutions for the most common issues with using Windows Update and explanations of error messages, see the Microsoft Update Solution Center at support.microsoft.com/ph/6527#tab3.

Although some of the services and processes described in this guide can be used to install non-security updates, this is not the focus because these updates typically are not required for security purposes.
For information about maintaining systems with all other update types, see [technet.microsoft.com/updatemanagement/](http://technet.microsoft.com/updatemanagement/).

**Security Update Policy for Non-Genuine Software**

Windows Update (Automatic Updates on Windows XP) will offer security updates for Windows and other Microsoft software to both genuine and non-genuine Windows computers. Non-genuine Windows systems can also install service packs, update rollups, and important reliability and application compatibility updates for Windows and other Microsoft software. This approach helps to keep the entire computer ecosystem safer because more systems are protected, regardless of whether they are genuine or not. However, at the discretion of Microsoft, other value-adding updates and software may be blocked for non-genuine systems.

On Windows 7 and Windows Vista, a non-genuine Windows system can access available updates through Windows Update Control Panel. On Windows XP, a non-genuine Windows system can only access security updates through Automatic Updates.

---

12 [www.microsoft.com/genuine](http://www.microsoft.com/genuine)
Glossary and Commonly Used Terms

This glossary helps explain the core concepts and technologies associated with the Microsoft Security Update Release and Deployment Process. For more information on malicious software terms, please visit the Microsoft Malware Protection Center (MMPC) portal. See www.microsoft.com/security/portal/encyclopedia.aspx.

active software security protections
Active software security protections can detect or defer intrusions into a Microsoft system or defend a Microsoft system from exploitation attempts, without the availability of a Microsoft security update for the issue being exploited (for example, antivirus definitions that trigger malicious behavior or IDS signatures that block exploitation attempts).

binaries
The two basic components of an update are the update binary (or binaries) and the update metadata file. The binary is the update executable, and a given update may include one or more update binaries. The update metadata file is an XML document that contains basic information about the update as well as when and how to install the update.

control
An organizational, procedural, or technological means of managing risk; a synonym for safeguard or countermeasure.

countermeasure
Software configurations, hardware, or procedures that reduce risk in a computer environment. Also called a safeguard or mitigation.

critical update
A broadly released fix for a specific problem, addressing a critical, non-security related bug, such as an update for the Microsoft Windows Malicious Software Removal Tool (MSRT).

Note: there are “Critical Updates” and security updates rated as Critical (in a Microsoft security bulletin). These are two different Microsoft updates. For more information about the differences, see the section above: “Microsoft Software Update Terminology”.

defense-in-depth
The approach of using multiple layers of security to guard against failure of a single security component.

denial of service
An explicit attempt to prevent legitimate users from using a service or system.
**elevation of privilege**
Where an unprivileged user gains privileged access. An example of privilege elevation would be an unprivileged user who contrives a way to be added to the Administrators group.

**exploit code**
A software program or sample code, that when executed against a vulnerable system, uses the vulnerability to spoof attacker identity, tamper with user or system information, repudiate attacker action, disclose user or system information, deny service to valid users, or elevate privileges for the attacker.

**feature pack**
A new product functionality usually included in the next full product release. Feature packs may include new security features and improvements.

**functioning exploit code**
Exploit code that is able to produce the maximum security impact of a vulnerability to occur. For example, if a vulnerability had a security impact of remote code execution, Functioning Exploit Code would be able to cause remote code execution to occur when run against a target system.

**hotfix**
A single package composed of one or more files used to address a problem in a product. Hotfixes address a specific customer situation, are only available through a support relationship with Microsoft, and may not be distributed outside the customer organization without written legal consent from Microsoft. The terms QFE (Quick Fix Engineering update), patch, and update have been used in the past as synonyms for hotfix.

**impact**
The overall business loss expected when a threat exploits a vulnerability against an asset.

**non-security update**
Any software update that is not security related. Microsoft specifically calls out non-security updates during the regular security update release cycle because some non-security updates, such as the Microsoft Outlook Junk Email Filter update, are released via Microsoft Update at the same time as the security updates.

**optional updates**
Optional updates can include updates, drivers, or new applications from Microsoft or its partners to enhance customer computing experiences. These updates need to be installed manually; that is, optional updates are not downloaded or installed automatically, but Windows Update provides them for review.
security update
A broadly released fix for a product-specific security-related vulnerability. Security vulnerabilities are rated based on their severity, which is assigned by the MSRC and indicated in the Microsoft security bulletin as critical, important, moderate, or low (severity ratings are discussed in detail earlier in this Guide).

service pack
A tested, cumulative set of hotfixes, security updates, critical updates, and updates, as well as additional fixes for problems found internally since the release of the product. Service packs might also contain a limited number of customer-requested design changes or features.

severity rating
A label Microsoft assigns to each vulnerability that helps customers assess the risks it poses to their organizations and compare it against other vulnerabilities when prioritizing deployments. Vulnerabilities can be designated as Critical, Important, Moderate, or Low.

software update
A software update is any update, update rollup, service pack, feature pack, critical update, security update, or hotfix that is used to improve or to fix a software product that is released by Microsoft Corporation.

supersedence
This term describes when a new security update in a security bulletin replaces another security update in an older security bulletin. In the case of supersedence, the binaries in the newer security update contain the fix for the current security vulnerability plus the fix for the older security update. In the past, new and previously released security updates, which contained the same fix, might have both been marked as required when the only one that was necessary was the newer security update.

update rollup
A tested, cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area such as security, or a component of a product. Among others, a good example of an update rollup is a Service Pack.

Windows Update Agent (WUA)
The Windows Update Agent (WUA) API is a set of COM interfaces that enable...
system administrators and programmers to access Windows Update and Windows Server Update Services (WSUS). Scripts and programs can be written to examine which updates are currently available for a computer, and then you can install or uninstall updates.

workarounds
The Workarounds section includes information on the workarounds that Microsoft has tested in order to help mitigate the threat until you have updated your environment. You must read this section as part of your risk assessment.