Trustworthy Computing

Software Vulnerability Management At Microsoft

July 2010
Contents

Introduction .......................................................... 4
High-Quality Security Updates ........................................ 11
  The Microsoft Development Process for Security Updates ........ 11
  Minimizing the Number of Security Updates ....................... 12
  Security Updates for All Affected Products Are Released Simultaneously ..................... 14
  Coordinated Security Update Releases .............................. 15
  Application Compatibility Testing ................................. 15
  Decreased Complexity and Time to Deploy Security Updates ........... 18
  Consolidated Security Updates to Minimize System Restart ........ 19
Community-Based Defense ............................................ 22
  Sharing Information and Intelligence with Partners ................ 22
  Sharing Research and Knowledge with Independent Software Vendors .................. 23
  Working with Security Researchers and Advocating for
  Coordinated Vulnerability Disclosure ............................. 24
Comprehensive Security Response Process .......................... 26
  Predictable and Transparent Release Cycle ......................... 27
  Communications and Guidance ..................................... 28
  Managing Risk through Standardized Workflow .................... 30
Conclusion ............................................................ 31
Contributors .......................................................... 32
Introduction

Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of that software or the data it processes. Some of the most severe vulnerabilities enable attackers to run software code of their choice, potentially compromising the system’s software. The disclosure of a vulnerability is the revelation of a vulnerability to the public at large. Disclosures can come from various sources, including software vendors, security software vendors, independent security researchers, and those who create malicious software (also known as “malware”).

It is impossible to completely prevent vulnerabilities from being introduced during the development of large-scale software projects. As long as human beings write software code, no software is perfect and mistakes that lead to imperfections in software will be made. Some imperfections (“bugs”) simply prevent the software from functioning exactly as intended, but other bugs may present vulnerabilities. Not all vulnerabilities are equal; some vulnerabilities won’t be exploitable because specific mitigations prevent attackers from using them. Nevertheless, some percentage of the vulnerabilities that exist in a given piece of software poses the potential to be exploitable.

Manual code reviews performed by developers and testers, in concert with automated tools such as fuzzers and static analysis tools, are very helpful techniques for identifying vulnerabilities in code. But these techniques cannot find every vulnerability in large scale software projects. As developers build more functionality into their software, their code becomes more and more complex. The challenge of finding vulnerabilities in very complex code is compounded by the fact that there are an infinite number of ways that developers can make coding errors that can create vulnerabilities, some of which are very, very subtle. To illustrate how subtle a security vulnerability can be, the following small code sample contains a vulnerability that is difficult to find using code reviews or tools or both.

```c
bool fAllowAccess = true;
if (AccessCheck(...) == 0 && GetLastError() == ERROR_ACCESS_DENIED)
    fAllowAccess = false;
```

In this real-world example, the developer who wrote the code intended to have the code check whether the user running the program should be denied access to the program or if they should be granted access.

The problem in this code is that the function (AccessCheck()) that the developer is using to decide whether to grant access to the user, can fail for many reasons, many of which are not conditions related to denying access. For example, if the application runs out of memory for any reason during this operation, the function could return an “out of memory” error instead of the “access denied” error that the developer was expecting. Because the developer only checks for an “access denied” error, this code will grant access to the user if any error other than “access denied” error is returned. This is, therefore, a vulnerability that could potentially be exploited if an attacker could create the right conditions.

Again, developers can make an infinite number of potential mistakes during software development. Many cannot be readily detected by human (individuals reviewing) or machine (through various code review tools and technologies) review. Some vulnerabilities are not identified because they aren’t known to be a vulnerability when the code is written; that is, security research continues to uncover new types of vulnerabilities that might affect products developed with the best practices available at the time.
Research in the Microsoft Security Intelligence Report (SIR) Volume 8\(^1\) shows that thousands of vulnerabilities of varying severities\(^2\) are disclosed continually across the entire software industry\(^3\) every year (see Figure 1).

![Industry-wide vulnerability disclosures by severity, by half-year from the first half of 2006 through the second half of 2009](image)

**Figure 1: Industry-wide vulnerability disclosures by severity, by half-year from the first half of 2006 through the second half of 2009**

Managing vulnerabilities within software is an industry-wide challenge—a challenge that must balance the flexibility of software design with consistency in coding practices. The customization of applications built on software platforms must be balanced with the wide variety of tools used to build and deploy solutions. Although thousands of disclosures are made throughout the software industry each year, the largest percentage of vulnerability disclosures relate to software applications. Figure 2 shows vulnerabilities for operating systems, browsers, and other components since the first half of 2006.

---

\(^1\) Microsoft Security Intelligence Report Volume 8, [www.microsoft.com/sir](http://www.microsoft.com/sir)

\(^2\) For an explanation of the Common Vulnerability Scoring System (CVSS) scoring methodology, see [http://www.first.org/cvss/cvss-guide.html](http://www.first.org/cvss/cvss-guide.html)

\(^3\) The nomenclature used to refer to different reporting periods is nHyy, where nH refers to either the first (1) or second (2) half of the year, and yy denotes the year. For example, 2H08 represents the period covering the second half of 2008 (July 1 through December 31), and 1H09 represents the period covering the first half of 2009 (January 1 through June 30).
Figure 2: Industry-wide operating system, browser, and other vulnerabilities during the period between the first half of 2006 through the second half of 2009

In general, trends for Microsoft vulnerability disclosures have mirrored those for the industry as a whole, though vulnerabilities in Microsoft software represent a small fraction of the total population as seen in Figure 3. Over the past four years, vulnerability disclosures relating to software manufactured by Microsoft have consistently accounted for 3 to 5 percent of all disclosures industry-wide.4

---

4 Microsoft Security Intelligence Report Volume 8, www.microsoft.com/sir
Software Vulnerability Management at Microsoft

Another way Microsoft tries to manage risk for its customers is through company efforts related to responsible disclosure (RD). Responsible disclosure means disclosing vulnerabilities privately to the vendor who created the software so that a comprehensive security update to address the vulnerability can be developed before the details become public knowledge. Ideally, with responsible disclosure, the release of the security update coincides with the public release of vulnerability information. This helps to keep users safer by limiting the risk that attackers would learn about newly discovered vulnerabilities before security updates are available. To reduce the risk of an attack to customers, Microsoft and others in the industry work to keep responsible disclosure rates as high as possible, using a variety of strategies to encourage reporting of vulnerabilities. Figure 4 shows responsible disclosures of vulnerabilities in Microsoft software that the Microsoft Security Response Center received in each half-year period since the first half of 2006, as a percentage of all disclosures.5

5 Microsoft Security Intelligence Report Volume 8, www.microsoft.com/sir
In July 2010, the Microsoft philosophy on the disclosure of vulnerabilities encouraging new levels of coordination between researchers and vendors, was announced, Coordinated Vulnerability Disclosure (CVD). CVD is an evolution of Responsible Disclosure that generally follows the same principles, in an effort to minimize risk to customers and minimize criminal activity on the Internet. It is important to note that no policy will eliminate risk, or criminal/malicious activity, however it is important to Microsoft customers that the focus always be on introducing less risk, and minimizing attacks.

The principles associated with Microsoft’s Coordinated Vulnerability Disclosure philosophy are as follows:

- Vendors and vulnerability finders need to work closely together toward a resolution
- Extensive efforts should be made to make a timely response
- Only in the event of active attacks is public disclosure, focused on mitigations and workarounds, likely the best course of action, and even then it should be coordinated as closely as possible.

Advocating for CVD helps Microsoft to galvanize the security community around a key point: that coordination and collaboration are required to resolve issues in a way that minimizes risk and disruption for customers. For more details on CVD and the way it is envisioned to work, see http://blogs.technet.com/b/ecostrat/archive/2010/07/22/coordinated-vulnerability-disclosure-bringing-balance-to-the-force.aspx.

Microsoft has also worked collaboratively with software companies through responsible disclosure, and now through coordinated vulnerability disclosure, to help identify vulnerabilities in other commercially available software by leveraging the tools and processes that Microsoft uses to review its own software. The Microsoft Vulnerability Research (MSVR) program is designed to improve the

---

6 http://go.microsoft.com/?linkid=9738193
security of software running on the Microsoft platform. Through the MSVR program, Microsoft extends its own security expertise and tools to discover vulnerabilities in third-party code that runs on the Microsoft platform, reports vulnerabilities to affected vendors, and then offers to assist the companies whose software has security vulnerabilities to resolve those vulnerabilities.

Another measure that suggests that the focus on responsible disclosure, and now coordinated vulnerability disclosure, benefits Microsoft customers is in the relatively low number of Microsoft “out-of-band” security updates. Microsoft implemented a predictable monthly security update release cycle in October 2003 whereby Microsoft releases security bulletins each month that fix vulnerabilities in Microsoft software. Security bulletins are typically released on the second Tuesday of each month, although on rare occasions Microsoft releases security updates between the monthly security updates (these are also known as “out-of-band” updates) when the vulnerability is determined to pose an urgent risk to customer systems.

Microsoft realizes that out-of-band security updates that address security vulnerabilities are unexpected and present planning and deployment difficulties for enterprise customers. With this in mind, Microsoft only releases out-of-band updates when the risk of exploitation using the vulnerability is determined to be elevated; these decisions are made by weighing the risk of exploitation and the potential impact to customers. Figure 5 shows the number of out-of-band security updates Microsoft released between 2005 and 2009 compared to regular security update releases during the same period.

<table>
<thead>
<tr>
<th>Period</th>
<th>Total Security Bulletins</th>
<th>Out-of-band Security Bulletins</th>
</tr>
</thead>
<tbody>
<tr>
<td>1H05</td>
<td>33</td>
<td>0</td>
</tr>
<tr>
<td>2H05</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>1H06</td>
<td>32</td>
<td>1</td>
</tr>
<tr>
<td>2H06</td>
<td>46</td>
<td>1</td>
</tr>
<tr>
<td>1H07</td>
<td>35</td>
<td>1</td>
</tr>
<tr>
<td>2H07</td>
<td>34</td>
<td>0</td>
</tr>
<tr>
<td>1H08</td>
<td>36</td>
<td>0</td>
</tr>
<tr>
<td>2H08</td>
<td>42</td>
<td>2</td>
</tr>
<tr>
<td>1H09</td>
<td>27</td>
<td>0</td>
</tr>
<tr>
<td>2H09</td>
<td>47</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>353</td>
<td>7</td>
</tr>
</tbody>
</table>

![Figure 5: Total security bulletins and out-of-band updates released by Microsoft between the first half of 2005 and the last half of 2009](image)

Despite the relatively low number of vulnerabilities in Microsoft products, historically high responsible disclosure rates and a low number of out-of-band security update releases, Microsoft understands that security vulnerabilities in Microsoft products still have the potential to disrupt customer experiences. In order 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...
Software Vulnerability Management at Microsoft

customers to understand the related risks posed to their information technology (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.7

Still, some security industry influentials 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 our priority at Microsoft for security updates is to minimize disruption to customers and to help protect against online criminal attacks.

The goal of this paper is to elaborate on the strategies employed by Microsoft to minimize disruptions to its customers. Although these insights apply to all Microsoft customers, this paper focuses on benefits to enterprise customers in particular.

For most consumers, the Microsoft Update service makes keeping Microsoft software up to date on their systems easy. Enterprises and organizations with large IT operations are often required to meet compliance requirements, standards, and guidelines. Subsequently these additional requirements demand a level of rigor and predictability that enterprise customers can rely on in order to minimize disruptions to their businesses.

In this paper, you’ll learn how Microsoft uses a multipronged approach to help its 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 Microsoft customers’ businesses.

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

---

7 Details on Microsoft’s security update release process and recommendations on how enterprise customers can leverage all of the outputs of this process are available in the Microsoft Security Update Guide available at [http://microsoft.com/securityupdateguide](http://microsoft.com/securityupdateguide)
High-Quality Security Updates

The challenge of minimizing disruptions to a diverse computing ecosystem of hundreds of millions of systems worldwide requires relentless focus on engineering excellence that leads to the development of high-quality products and, as needed, corresponding high-quality updates for those products. This section of this paper focuses on Microsoft security update releases and some of the ways the company works to minimize disruptions to enterprise customers’ operations, keep associated costs for customers low, and help provide protection from online criminal activity. To do this, Microsoft rigorously designs, develops, and tests comprehensive security updates with a focus on deployment ease for customers.

This section discusses several related topics including the process that Microsoft uses to develop security updates, Microsoft efforts to minimize the number of security updates, the importance of releasing security updates in a simultaneous and coordinated fashion, some insights into functional testing and application compatibility testing for Microsoft security updates, and some ways Microsoft works to make it easier for enterprises to deploy security updates.

The Microsoft Development Process for Security Updates

When a security researcher finds a vulnerability in Microsoft software and reports it to Microsoft, the Microsoft Security Response Center (MSRC) uses a process to manage the investigation, development, and release of a security update for the vulnerability. This process is comprehensive to ensure that security updates released by Microsoft address the vulnerabilities identified with minimal disruption to the hundreds of millions of customers using Microsoft software around the world.

The process of investigating and developing a security update includes several related categories of work:

- **Triage and reproduction:** Reproduce the issue, assess its severity, identify the root cause, determine affected components and products, identify and test existing mitigations, and determine if a new security update should be released.
- **Planning:** Assess whether new functional testing needs to be conducted and determine how vulnerability variant investigation will occur, identify appropriate release mechanism and target release date.
- **Finding variants:** Create fuzzing tools and/or improve existing ones to ensure proper coverage to identify related issues, identify new variants, review code fixes/assembly from a security perspective, (when applicable) run static code-analysis tools to help identify any unidentified issues.
- **Code and engineering reviews:** Perform engineering reviews to ensure the code change addresses the underlying issue and determine the broader impact of the code change.
- **Functional testing:** Ensure code changes have not affected functionality in an unexpected way; setup and deployment testing as well as serviceability testing is performed for all affected platforms.
- **Integration testing:** Application compatibility testing and working with partners (other groups within Microsoft and ISVs) that are potentially affected by the vulnerability or the security update or both.
The comprehensive nature of a vulnerability investigation and subsequent engineering work takes time. Although some of the categories of work described above can be completed simultaneously, some of the work cannot be rushed without increasing the risk of disruptions—for example, application compatibility issues—for customers.

Some of the benefits and challenges related to this process are discussed in more detail in the remainder of this section.

Minimizing the Number of Security Updates

The MSRC receives more than 100,000 email messages per year (273 email messages per day or 11 per hour, from approximately 0.01% of customers using computers and devices running Windows) at secure@microsoft.com. Most of this email is from customers that have encountered a security issue but are not reporting a vulnerability. For example, customers need help logging into Windows Live Hotmail or something similar. In these cases, the MSRC routes them to the correct support team within Microsoft for help. However, some of these email messages are from security researchers and passionate customers located all over the world who believe they might have identified a vulnerability in a Microsoft product. Security experts read and monitor every email message manually and are continually on the alert for information about newly discovered vulnerabilities.

---

The MSRC opens an investigation to determine if a reported vulnerability exists and what components and products the vulnerability affects. After a vulnerability has been confirmed, the development process for security updates described above is initiated.

This comprehensive approach to investigations and fixing vulnerabilities helps avoid the need to re-release a security update or to release multiple updates to address issues in the same components that otherwise could have been addressed in a single update. This type of scenario occurred when Microsoft released security bulletin MS03-026 on July 16, 2003. After the update was released, three additional vulnerabilities were discovered in the same component: RPCSS/DCOM. MS03-039 was then released to address all vulnerabilities in the component on September 10, 2003. Identifying variants of vulnerabilities in code is often difficult and time-consuming. For example, in some cases, new fuzzing techniques and/or new tools need to be developed so that security engineers can perform the meticulous testing required to ensure a high level of confidence that all variants of a vulnerability have been identified and addressed. After ensuring that the reported vulnerability and any variants have been addressed and testing the update, deep functional testing, setup and deployment testing, serviceability testing, and application compatibility testing are all completed to ensure the highest quality security update possible is ready for release. It is important to note that once a security update is released, the update will be deployed to hundreds of millions of systems worldwide in a very short period of time. Given the scale of deployment required, it is imperative that the update has been rigorously engineered to avoid creating any type of disruption to these systems.

Throughout the testing, the MSRC monitors the threat landscape for signs that the vulnerability or variants are being used in active attacks. The MSRC does this by using comprehensive telemetry systems as well as data and information provided by customers and partners around the world, along with relationships with the security industry. This approach helps Microsoft balance the potential urgency of releasing an update for a vulnerability that is under active exploitation with the need for high confidence that the update will address the vulnerability and all of its variants and maintain the functionality and stability that customers expect from the affected products.

Microsoft tries to address vulnerabilities and all of their variants in as few updates as possible. Deploying updates costs enterprise customers time, effort, and money. Therefore, costs increase if customers have to re-assess the effects and deploy multiple updates. Taking additional time to complete a comprehensive examination helps to ensure the number of security updates Microsoft releases and might need to re-release, is kept to a minimum, thus reducing the costs and potential disruption to enterprise customers’ operations. With the increased quality of security updates achieved over the last five years, some enterprise customers deploy security updates with little or no testing, and hundreds of millions of consumers continue to use the Automatic Update clients on their Windows systems to ensure that they stay protected automatically.
Security Updates for All Affected Products Are Released Simultaneously

One principle that Microsoft uses to help customers manage risk is to offer security updates for all products affected by a given vulnerability simultaneously. When a software vulnerability is reported to Microsoft, the MSRC opens an investigation to determine if the reported vulnerability exists and what components and products the vulnerability affects. In some cases a vulnerability exists in a single product, but in many cases, a single reported vulnerability is shared by multiple components and/or products. For example, security bulletin MS04-028\(^\text{11}\) (published September 14, 2004), addressed a vulnerability in GDI+ that affected fifty-three separate products. Identifying all components and products, including applicable third-party products, that are affected by a vulnerability is a critical step in an MSRC investigation. The work to do this is not trivial from an engineering perspective because code in different products and components is modified from release to release. Often, the result is that a single reported vulnerability is identified as a variant in earlier version products. Variants typically require different fixes that all must be tested differently.

Some have argued that to release security updates more quickly, Microsoft should release security updates as they become ready and not try to release updates for all affected products simultaneously. They argue that the time it takes to fully investigate the code in all potentially affected components and products exposes the computing ecosystem to increased risk.

When Microsoft releases a security update, security researchers and criminals immediately start reverse engineering the security update in an effort to identify the specific section of code that contains the vulnerability being fixed. Once they identify the vulnerability addressed by the update, they attempt to develop code that will allow them to exploit that vulnerability on systems that do not have the security update installed on them. They also try to identify whether the vulnerability exists in other products with the same or similar functionality. For example, if a vulnerability is addressed in one version of Windows, researchers investigate whether other versions of Windows have the same vulnerability. In the past, some researchers have been able to develop working exploit code for some vulnerabilities in a matter of days or even a few hours.

If Microsoft released security updates for affected products in a staggered manner instead of releasing updates for all affected products simultaneously, this would extend the window of opportunity that criminals can use to attack Microsoft customers, increasing the risk for customers. In the case of MS04-028 mentioned earlier in this paper, if Microsoft hadn’t released security updates for all the products that shared the same vulnerability at the same time, it would have increased the likelihood that attackers would have successfully attacked affected products that were not updated in the initial update release. Such a process would provide an advantage to criminals and disadvantages to customers.

Some critics of this process lament that the Microsoft pledge to provide security updates for older versions of affected software (also known as “legacy code”) slows down the release of security updates for newer products. Microsoft customers benefit from one of the longest product support lifecycle policies in the software industry. One major advantage of the support lifecycle policy includes continued security update support throughout the lifetime of the product. Typically this provides 10 years of support for many products (5 years Mainstream Support and 5 years Extended Edit 11\) http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx
Software Vulnerability Management at Microsoft

Support). This product-support-lifecycle policy helps protect enterprise customers and the entire ecosystem by providing security update support for the many versions of Windows-based systems in the ecosystem. For example, support for Windows 2000, which was originally released on March 31st 2000, ended on July 13, 2010. The support lifecycle policy provides enterprise customers with the time and flexibility needed to maximize the return on investment from their applications running on Microsoft software and to minimize the total cost of ownership, while maintaining their ability to manage risks during the same period.

Coordinated Security Update Releases

There are security vulnerabilities that affect many applications developed by different software vendors across the ecosystem. Addressing these types of vulnerabilities requires far more coordinated work among Microsoft, its partners, and the broader software industry than other types of vulnerabilities. As a result, it takes significantly more time to investigate, identify the attack vectors, develop mitigations and engineer a solution that helps protect the entire ecosystem, and release and deploy associated security updates. These cases can involve many third parties, not all of which have well developed incident response mechanisms in place.

For example, in 2008, a security researcher discovered a vulnerability in the Domain Name System (DNS) protocol that allows all Internet users to resolve domain names to IP addresses. Because this vulnerability was introduced in the design specifications that all software vendors use when they develop DNS related code, this vulnerability affected several major software vendors’ implementations of DNS. Several major software vendors with affected products and services subsequently released security updates to address this vulnerability, including Microsoft, who released Security Bulletin MS08-037. To help protect all users of the Internet and avoid giving criminals an advantage, the affected vendors worked together on coordinated releases of updates to address this problem.

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.
Figure 7: An illustration reflecting the size of an example test matrix containing a subset (for the purposes of example) of tested languages and applications.
This large test undertaking to address multiple architectures, products, and versions is a key way that Microsoft minimizes disruptions to enterprise customers. To further minimize the potential for disruption, in 2005, Microsoft started the Security Update Validation Program (SUVP). The SUVP seeks to ensure the quality of security updates by testing them in environments, configurations, and against applications (such as line-of-business 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.

The efforts outlined above 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, returning budget to fund other projects or reducing operating expenses to their corporations.

**Decreased Complexity and Time to Deploy Security Updates**

The time spent developing, testing, and releasing security updates (including the detection logic needed to determine whether each individual system around the world needs to be offered any given update) through Windows Update and Microsoft Update enables Microsoft to provide security updates to hundreds of millions of diverse systems worldwide quickly and securely. This helps enterprises manage risks in their IT environments by dramatically decreasing the time and effort it takes to assess and deploy security updates for Microsoft software.

Before the release of the Windows 98 operating system, security updates from Microsoft were released using the Microsoft Download Center. Administrators had to manually download and install security updates for Windows and Microsoft products after they determined whether the update applied to any of the products they ran in their environments. This was not a trivial task for administrators to undertake; therefore, the security deployment practices of many enterprises were sub-optimal.

For example, a vulnerability in Microsoft SQL Server 2000 addressed in Microsoft Security Bulletin MS02-039 was originally released on the Microsoft Download Center because it pre-dated the availability of the Windows Update Service and Automatic Update Client. At this time, many administrators were unaware that they needed to install the update. Compounding the challenge, the steps required to install the update manually were hard to follow, and administrators had no tools to find systems running affected components in their environments. Although the security updates

---


update that addressed the vulnerability was released on July 24, 2002, the “SQL Slammer” worm successfully exploited the vulnerability on numerous systems around the world starting January 25th, 2003 (six months later). Many businesses were disrupted as a result of this attack.

The Windows Update service and the Automatic Update Client revolutionized security updating by automatically determining whether individual Windows systems required each security update released by Microsoft based on the components installed on each system. These innovations drastically reduced the complexity and time required to assess and install security updates for Microsoft software, helping to protect the computing ecosystem more efficiently and effectively. Windows Update, and later Microsoft Update, along with tools such as Microsoft Baseline Security Analyzer (MBSA), Windows Server Update Services (WSUS), Microsoft System Center Configuration Manager, Systems Management Server 2003 Inventory Tool for Microsoft Updates, and others\textsuperscript{17} helped enterprise customers save time, effort, and costs associated with doing such work manually\textsuperscript{18}.

The Microsoft Update service, launched June 2005, provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when they install software serviced through Microsoft Update or at the Microsoft Update website\textsuperscript{19}. Two key features of the Automatic Update Client are delta binary patching and background processing. These features allow enterprise administrators to download a full package to their WSUS server, while the desktops on the network only download the specific components of the package necessary to implement the update. These features play a major role in reducing network and branch office traffic related to downloading Microsoft security updates, and it minimizes the impact to information workers who are working on desktops during deployments. Today, the efficiencies these innovations provide are necessary to help keep Microsoft customers ahead of online criminal attackers who seek to disrupt their businesses for profit\textsuperscript{20}.

**Consolidated Security Updates to Minimize System Restart**

Microsoft recognizes that restarting systems can disrupt its customers’ businesses and that uptime is critical. Restarting systems after installing Microsoft security updates is only required when absolutely necessary. There have been suggestions that Microsoft release fewer, larger update packages containing all necessary updates to reduce the number of system restarts required.

The MSRC is constantly trying to find ways to reduce system restart requirements for security updates, while it manages a broad set of considerations. A single security bulletin often addresses multiple vulnerabilities from the Common Vulnerabilities and Exposures (CVE) database\textsuperscript{21}, each of which is listed in the bulletin, along with any other relevant issues. The figure below shows the number of security bulletins released and the number of individual CVE-identified vulnerabilities they have addressed for each half-year period since 1H05\textsuperscript{22}. (Note that not all vulnerabilities are addressed in the period in which they are initially disclosed.)

\textsuperscript{17} http://technet.microsoft.com/en-us/security/cc297183.aspx
\textsuperscript{18} http://microsoft.com/securityupdateguide
\textsuperscript{19} http://update.microsoft.com/microsoftupdate
\textsuperscript{20} http://microsoft.com/sir
\textsuperscript{21} http://cve.mitre.org
\textsuperscript{22} Microsoft Security Intelligence Report Volume 8, www.microsoft.com/sir
Whenever possible, the MSRC consolidates multiple vulnerabilities that affect a single binary or component and addresses them with a single security bulletin, to maximize the effectiveness of each update and minimize the potential disruption that customers face from testing and deploying individual security updates into their computing environments. When vulnerabilities affect different unrelated components and must be addressed by separate updates, consolidation is not always feasible. Although the ratio of CVEs to security bulletins in 2H09 is down from the historic high achieved in the first half of the year, the ratio remains high in relation to most previous periods, and the overall trend is positive\textsuperscript{23}.

\textsuperscript{23} Microsoft Security Intelligence Report Volume 8, \url{www.microsoft.com/sir}
Figure 9: Average number of CVEs addressed per security bulletin from the first half of 2005 through the second half of 2009
Community-Based Defense

Security is a challenge for the entire industry and one that no single company can solve by itself. As the data in the introduction of this paper illustrates, thousands of security vulnerabilities are disclosed across the software industry each year, most in applications, and most of a high severity. Microsoft works with partners and the broader industry in a variety of ways to sustain resilient computing environments around the world. Much of the information that an MSRC vulnerability investigation generates is not only used to engineer a security update to address the vulnerability and provide tested guidance for customers, but also to enable a large number of Microsoft partners to protect their customers. Enabling partners is a cornerstone of the Microsoft security strategy—one that benefits a wide variety of organizations and consumers. The ultimate goal of this work is to minimize disruptions and to continuously improve the capabilities of computers and devices to withstand disruption, attack, and theft in a variety of forms.

Sharing Information and Intelligence with Partners

Microsoft operates and/or participates in several software vulnerability sharing programs.

The Microsoft Active Protections Program\(^{24}\) (MAPP) is a program for security software providers. Members of MAPP receive vulnerability information early so that they can provide timely, updated protections to enterprise customers through their security software or devices, such as antivirus software, network-based intrusion detection systems, or host-based intrusion prevention systems.

The MAPP partner page includes links to the active protections partners (www.microsoft.com/security/msrc/mapp/partners.mspx). The result for enterprise customers is enhanced protections from vendors they trust that they can deploy while they test and deploy Microsoft security updates.

Recognizing the important role the security response community plays in Microsoft security efforts, the company formed the Microsoft Security Response Alliance (MSRA) in 2006 as a framework for partners, vendors, governments, and infrastructure providers to collaborate in a secure and timely manner. The MSRA serves as an “umbrella” structure for a number of other alliances and initiatives, several of which pre-date the formation of the MSRA itself. For example, the Microsoft Virus Initiative (MVI) was originally formed in 1997 to facilitate communication between Microsoft and antivirus (AV) software vendors about macro viruses, which led to the development of the Antivirus application programming interface (Antivirus API). Figure 10 lists the MSRA member organizations and their primary businesses.

\(^{24}\) www.microsoft.com/security/msrc/collaboration/mappfaq.aspx
<table>
<thead>
<tr>
<th>Organization</th>
<th>Focus</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Global Infrastructure Alliance for Internet Safety (GIAIS)</td>
<td>Internet service providers (ISPs)</td>
<td>Fosters cooperation between Microsoft and the world’s leading ISPs to keep their customers safe on the Internet</td>
</tr>
<tr>
<td>The Microsoft Virus Initiative (MVI)</td>
<td>Security researchers, antivirus software vendors</td>
<td>Enables Microsoft to share key technical details of Microsoft technologies with partners, to facilitate development of well-integrated security solutions</td>
</tr>
<tr>
<td>Virus Information Alliance (VIA)</td>
<td>Antivirus software vendors</td>
<td>Provides AV partners with detailed technical information about significant viruses affecting Microsoft products and customers</td>
</tr>
<tr>
<td>Microsoft Security Cooperation Program (SCP)</td>
<td>Public sector infrastructure, law enforcement, public safety, and education</td>
<td>Provides a framework for information exchange and collaboration between Microsoft and the public sector, primarily in the areas of response and outreach</td>
</tr>
<tr>
<td>Microsoft Security Support Alliance (MSSA)</td>
<td>Microsoft original equipment manufacturer (OEM) partners</td>
<td>Provides authoritative and timely information on newly discovered security threats to Microsoft’s OEM partners, enabling them to better communicate security information to their customers</td>
</tr>
<tr>
<td>Security Alliance for Financial Institutions (SAFI)</td>
<td>Financial institutions</td>
<td>Facilitate collaboration between Microsoft and financial institutions worldwide regarding the threats that such institutions face</td>
</tr>
</tbody>
</table>

**Figure 10: Organizations and working groups under the MSRA umbrella**

For more information about MSRA, see [http://www.microsoft.com/security/msra/default.mspx](http://www.microsoft.com/security/msra/default.mspx)

The Industry Consortium for the Advancement of Security on the Internet (ICASI)\(^25\), of which Microsoft is a founding member, is a trusted forum for addressing international, multi-product security challenges. This trusted forum extends the ability of information technology vendors to proactively address complex security issues and better protect enterprises, governments, and citizens, and the critical IT infrastructures that support them. ICASI shares the results of its work with the IT industry through papers and other media.

**Sharing Research and Knowledge with Independent Software Vendors**

The Microsoft Vulnerability Research (MSVR) program was announced in 2008. This program is intended to make use of Microsoft knowledge and experience in securing software to help other software and hardware vendors deal with vulnerabilities reactively as well as develop proactive internal programs to improve the overall security of their products.

\(^25\) [http://www.icasi.org/index.htm](http://www.icasi.org/index.htm)
The goals of the MSVR program include:

- **Research**: Find vulnerabilities in third-party software running on the Windows platform, either manually or through the use of internally developed tools.

- **Coordination**: Provide information about internally discovered vulnerabilities to the developers of the affected software and to other organizations that can help address the issues.

- **Protection**: Work with software vendors to help protect customers by taking advantage of security functionality built into the Windows platform, such as Internet Explorer ActiveX control kill bits and the proactive use of Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).

- **Engineering Excellence**: Coordinate with the SDL Outreach team to help evangelize the advantages of Microsoft’s Security Development Lifecycle (SDL) and help vendors move towards more secure and proactive development processes.

### Working with Security Researchers and Advocating for Coordinated Vulnerability Disclosure

Microsoft collaborates with many other parties when it investigates potential vulnerabilities in Microsoft software. Microsoft looks to mitigate exploitation of vulnerabilities through the capabilities of the industry, partners, public organizations, customers, and security researchers. Along the way, Microsoft supports and encourages coordinated vulnerability disclosure (CVD) of vulnerabilities. As mentioned earlier in this paper, Coordinated Vulnerability Disclosure means vendors and vulnerability finders work closely toward a resolution; extensive efforts are made to make a timely response; and only in the event of active attacks is public disclosure, focused on mitigations and workarounds, the best course of action, and even in those instances should be coordinated as closely as possible. The goal of CVD is to encourage the coordination and collaboration in the security community necessary to resolve issues in a way that minimizes risk and disruption for customers. Ideally, with CVD, the security update is released to coincide with public availability of the vulnerability information. This process serves everyone’s best interests and ensures that users are not exposed to malicious exploitation while security updates are being developed.

When a security researcher is acknowledged in a Microsoft monthly security bulletin, the acknowledgment signals that the vulnerability was reported to the MSRC using CVD practices and that the individual security researcher or organization worked with Microsoft to help the company understand the vulnerability, the extent of the risk to the products and platforms, and possible mitigations. During the technical investigation and development of the update, the vulnerability reporter is continually apprised and updated about the availability of the impending security update. In the end, this process helps provide a solution for deployment across customer systems before potential attackers are aware of the vulnerability or are able to leverage the vulnerability for malicious use.

In many cases, a researcher reporting a vulnerability to Microsoft has invested time and effort to uncover and detail the vulnerability in question. After the vulnerability is reported, it is understandable that a researcher is interested in seeing their discovery communicated externally as soon as possible. Yet, as this paper has described, an MSRC investigation includes looking for variants of a reported vulnerability, inspecting the related code around a reported vulnerability, and
looking for the vulnerability in other components and products that share similar functionality. Investigations might also include working with multiple third parties, such as ISVs, to address related issues in intellectual property that they own. These stages, across the size of the installed base and affected version or versions along with third-party product implications and feedback loops through security partner programs all contribute to quality updates but extend the time to fix. The length of time between the report of a vulnerability in Microsoft software and the release of a security update has been mentioned as a point of disagreement by those who would like to see all discovered issues fixed quickly. Some researchers have chosen to release details of a discovered vulnerability before a security update has been completed. This course of action can expose the ecosystem to greater risk and can lead to active attacks on consumers and enterprises alike.

Microsoft takes action on both privately and publicly reported issues. Since uncoordinated vulnerability disclosure can lead to more attacks on customers, the risks of using uncoordinated vulnerability disclosure do not outweigh the benefits of collaboration. Microsoft continues to stand by its position that coordinated vulnerability disclosure—when reporting vulnerabilities to Microsoft or to any software vendor—is the most prudent and constructive course of action.

Security researchers that report vulnerabilities to Microsoft live and work all over the world. Consequently, security-related conferences and events are held all over the world. The MSRC sponsors, attends, and delivers presentations at many of these conferences and events. Engaging in the security community by supporting worldwide events helps Microsoft learn about the new areas of focus and industry trends within the security community, tools and techniques, and related cultural and philosophical elements that affect the security landscape. The conferences are a platform for technical information exchange, for new research and relationships to be developed, and for greater understanding of regional trends and research. Attending these events ultimately helps the MSRC provide timely and accurate information that helps better protect customers. These events are also an opportunity for the MSRC to give something back to the security community by presenting technical content related to vulnerabilities, tools, and more. The MSRC sponsors only those security conferences where there is a strict adherence to CVD practices.
Figure 11: Conferences that the Microsoft Security Response Center sponsored and/or attended between 2005 and 2009.
Comprehensive Security Response Process

Over the past decade, the computing ecosystem has been disrupted by major attacks several times. In response to these attacks, Microsoft has built a comprehensive security response process to help minimize disruptions to customers. This process includes a predictable and transparent release cycle for security updates that includes the timely publication of customer-focused communications and guidance. This process also includes managing risk for the computing ecosystem through a standardized workflow at Microsoft called the Software Security Incident Response Process, described in this section of this paper.

Predictable and Transparent Release Cycle

Beginning in October 2003, Microsoft started releasing security bulletins to address discovered vulnerabilities in Microsoft software on a predictable, monthly schedule. Since then, security bulletins have been released on the second Tuesday of each month. The bulletins provide a standard list of details to help customers understand and assess the risk to their computing environment posed by the vulnerabilities documented in each bulletin and understand how these vulnerabilities can be addressed.

Implementing a predictable monthly release schedule was a direct result of feedback from Microsoft enterprise customers; the insight from this feedback was that monthly security update releases work best for enterprise customers. The predictable monthly cadence makes it easier for enterprise administrators and operations teams to plan, resource, schedule, and budget for the deployment of security updates. A monthly cadence provides a reasonable amount of time for large enterprises to evaluate, test, and deploy security updates in their environments.

Some consider this predictable monthly release cycle too slow and suggest that it exposes enterprises to greater risk. Before October 2003, Microsoft did not release security updates on a predictable monthly cycle. Any number of security updates was released weekly, as soon as they were ready for release. For example, between June and August 1998 twelve separate security updates were released. Today, only three updates would be released over the same period of time.

The unpredictable nature of this process made it difficult for enterprise customers to plan, resource, schedule, and budget for deployments. Before October 2003, some of these customers developed their own risk assessment and deployment methodologies that had a monthly or quarterly cadence to help them manage deployments in a way that could be planned, resourced, scheduled, and budgeted for. Although this approach enabled these customers to better plan deployments, it provided a head start to attackers because of the window of opportunity between the time the security update was publicly released and the time the update was deployed. Many other customers simply couldn’t manage such an unpredictable release process and abandoned deploying security updates in favor of accepting more risk and deploying service packs on a much longer timeline. Some customers that could not tolerate the same risk levels tried to keep pace with the rapid, ad hoc release schedule but found that it became expensive to properly resource and budget for this work. Some customers told Microsoft that even if security updates were released the same day each week, this frequency was simply too difficult to manage, and they requested a better approach.

For the same reasons, Microsoft tries to minimize the release of out-of-band security update releases. Today, nearly seven years after implementing the predictable monthly security update release cycle, Microsoft receives feedback from enterprise customers that this release cycle continues to help
them effectively manage risks, minimize disruptions, and optimize their operations. Over time, several other major software companies with large enterprise customer install bases, such as Adobe (http://blogs.adobe.com/asset/), also adopted predictable security update cycles for their customers.

**Communications and Guidance**

In addition to providing customers with security updates to help protect them, Microsoft also provides communications that help keep customers informed about risks, detailed guidance that helps them assess risks and informs deployment strategies, and support options for when customers need help and advice.

When there is relevant information about a vulnerability that threatens the security of its products, Microsoft sends out notifications to customers. The breadth and depth of the communications that Microsoft produces is based on direct customer feedback on the type of information customers need and when they need it. Microsoft simultaneously publishes communications about security updates, localized in many different languages.

This consistent, predictable approach enables enterprise customers around the world to take advantage of security vulnerability information and deployment guidance when they are assessing risks and deployment strategies. The technical information provided in these communications has been written and reviewed by the appropriate security professionals across Microsoft. Information is the most important resource for enterprise customers during a security update release; without timely information and mitigations and workarounds, Microsoft enterprise customers could not accurately assess risks or deploy security updates in their environments with the high level of confidence they require.

The Microsoft Security Bulletin Advance Notification Service (ANS) helps enterprise customers plan the appropriate resources for an impending security update release. An 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 security updates are released by not disclosing any information that could facilitate attacks.

To help ensure against surprises and to minimize possible confusion and disruption, 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 Malicious Software Removal Tool (MSRT). Where possible, Microsoft makes this notice available three business days before a security bulletin is released to give administrators and operations teams time to plan for the release without giving attackers an advantage.


When security bulletins are released, the security bulletin advance notification is replaced by the security bulletin summary, providing the definitive resource for information about the security

---

26 http://www.microsoft.com/technet/security/bulletin/advance.mspx
Software Vulnerability Management at Microsoft

update. 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 professionals with risk evaluation. In addition to the information in the advance notification, security bulletin summaries contain an assessment of each vulnerability’s potential exploitability. The Exploitability Index\textsuperscript{27} was developed based on customer feedback to help IT professionals prioritize deployment of security updates based on the likelihood of exploitation. For more information about Microsoft security bulletin summaries, see www.microsoft.com/technet/security/bulletin/summary.mspx.

Each security bulletin contains detailed guidance and information about the security update and the vulnerability. Security bulletins are localized in 14 languages\textsuperscript{28}, and contain frequently-asked questions, vulnerability information, mitigations and workarounds, and other pertinent security update information. Security bulletin summaries are provided in 5 additional languages\textsuperscript{29}. For more information, see the Microsoft Security Bulletin Search page at www.microsoft.com/technet/security/current.aspx.

The Microsoft Customer Service and Support (CSS) group 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.

Microsoft security advisories, localized in 18 languages\textsuperscript{30}, are communications from Microsoft about potential vulnerabilities, active attacks, and other security information that is material to an IT installation’s overall security needs. Some security advisories may result in the release of a security update or may include guidance to help IT professionals mitigate the threat that is posed. Some notifications may not require a security bulletin or a security update, but may still affect customers’ overall security. 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:

\begin{itemize}
  \item Guidance and mitigations that may be applicable for publicly disclosed vulnerabilities.
  \item Clarifying information about potential threats that are publicly disclosed.
\end{itemize}

In addition, security and privacy experts at Microsoft share further insights, information, guidance, and knowledge in numerous blogs dedicated to security and privacy topics, including security update releases. To make it easier to consume all of the information published across all of these blogs, a “blog aggregator” page dynamically consolidates and features this blog content. You can access the Trustworthy Computing Security and Privacy blog aggregator at www.microsoft.com/twc/blogs.

\textsuperscript{27} http://technet.microsoft.com/security/cc998259.aspx
\textsuperscript{28} Languages include Chinese Traditional, Chinese Simplified, Dutch, French, German, Hungarian, Italian, Korean, Polish, Portuguese, (Portugal), Portuguese (Brazil), Russian, Spanish, Turkish
\textsuperscript{29} Languages include Czech, Danish, Finnish, Hebrew, Norwegian
\textsuperscript{30} Languages include Chinese Traditional, Chinese Simplified, Czech, Danish, Dutch, French, German, Hebrew, Hungarian, Italian, Korean, Norwegian, Polish, Portuguese, (Portugal), Portuguese (Brazil), Russian, Spanish, Turkish
Managing Risk through Standardized Workflow

When a security incident threatens Microsoft customers—whether it is an attack on the entire Internet or is more restricted in scope—the MSRC quickly mobilizes teams across Microsoft and around the world, including affected product teams, Customer Support and Services, Microsoft IT, and external partners. The MSRC uses the Microsoft worldwide Software Security Incident Response Process (SSIRP) to understand security incidents, that is, a situation that arises where malicious users exploit vulnerabilities. The SSIRP enables Microsoft to quickly investigate, analyze, and resolve those incidents. SSIRP has several phases:

- **Watch**: MSRC and its partners are always on the alert for threats.
- **Alert and mobilize resources**: When a threat is identified, first responders are paged and mobilized into two teams of engineers and communications professionals.
- **Assess and stabilize**: The engineering team investigates and develops the solution, and the communications team reaches out to provide guidance to customers and partners.
- **Resolve**: MSRC provides tools and solutions, and the Watch phase resumes.

Microsoft SSIRP participants include the MSRC\(^{31}\), the MMPC\(^{32}\), the MSEC\(^{33}\), and Microsoft product groups—such as the Windows, Internet Explorer, SQL Server, and Microsoft Office teams. Collectively, these groups provide visibility on active attacks by using data from massive telemetry systems they manage\(^{34}\). In addition, SSIRP participants also include external partners and organizations like the GIAIS (a consortium of Internet Service Providers), VIA (an alliance where partners exchange valuable technical information on newly discovered viruses), and the MVI (a forum designed to share information and improve responses to virus outbreaks)\(^{35}\).

Microsoft leverages its SSIRP capabilities to help balance the urgency required to release a security update and the time required to perform all of the actions outlined in this paper, including using a predictable and transparent release cycle that provides customer-focused communications and guidance, releases high quality updates and leverages community-based defense to increase the scale of protections for customers. Ultimately, the goal of all of these efforts is to minimize disruptions to customers’ businesses.

---

\(^{31}\) [http://microsoft.com/msrc](http://microsoft.com/msrc)

\(^{32}\) [http://www.microsoft.com/mmpc](http://www.microsoft.com/mmpc)

\(^{33}\) [http://www.microsoft.com/msec](http://www.microsoft.com/msec)

\(^{34}\) Telemetry systems as documented in the Microsoft Security Intelligence Report [www.microsoft.com/sir](http://www.microsoft.com/sir)

Conclusion

It is impossible to completely prevent the introduction of vulnerabilities during the development of large-scale software projects. Microsoft uses a multipronged, customer-centric strategy to help minimize disruptions to customers that includes:

- **High-quality security updates**—Using world class engineering practices produces high-quality security updates that can be confidently deployed to hundreds of millions of diverse systems in the computing ecosystem and helps 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 Microsoft’s customers’ businesses.

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

Microsoft and the security engineers, product managers, program managers, and communications professionals it employs continue to be dedicated to creating secure, private, and reliable computing experiences for everyone.
Contributors

Adrian Stone  
Microsoft Security Response Center

Adrienne Hall  
Microsoft Trustworthy Computing

Baris Saydag  
Microsoft Windows Serviceability

Damian Hasse  
Microsoft Security Response Center

David Hicks  
Microsoft Windows Compatibility

Hemanth Kaza  
Microsoft Windows Compatibility

James Rodrigues  
Microsoft Windows Serviceability

Jeff Jones  
Microsoft Trustworthy Computing

Mark Miller  
Microsoft Trustworthy Computing

Mike Reavey  
Microsoft Security Response Center

Matt Thomlinson  
Microsoft Security Response Center

Paul Potterff  
Windows Consumer Product Management

Sue Bohn  
Microsoft Windows Compatibility

Tim Rains  
Microsoft Trustworthy Computing