Microsoft Patch Management

A Guide for IT Professionals

wanstor

Contents

wanstor

Introduction

Patch management is a critical part of maintaining the security of your IT systems and network. The patch management system that you build and maintain is one of the main channels through which you deploy security updates from Microsoft and other vendors.

Although patch management is sometimes viewed as a systems management discipline rather than a security discipline, its role in addressing potential vulnerabilities through the deployment of updates makes it a vital component in a business's IT security operations.

At Wanstor we understand that the timely application of security updates is one of the most important and effective things an IT Manager can do to protect systems and the network.
Therefore a patch management system must be as efficient and effective as possible to stop security threats before they happen.

To help customers develop and maintain efficient and effective patch management strategies, Wanstor has developed this document specifically to help with Microsoft patch management. The reason we have produced a document specific to Microsoft is because this vendor is the dominant operating system in most organisations today.

This article will help IT Managers in business and not for profit organisations of all sizes with their patch management strategy and approach.

With a better understanding of core principles around Microsoft patches, IT Managers will be able to improve the efficiency of their patch management processes and prevent unpleasant surprises that can result from pursuing a strategy that Microsoft doesn't recommend or support.

Finally, with an understanding of the "why" behind how we recommend customers implement Microsoft patch management, should help to answer questions that may arise in an IT Managers day-to-day work managing security updates for Microsoft products.

wanstor

Service packs are the foundation of a good patch management strategy

We recommend IT Manager's view Microsoft service packs as the primary means for security maintenance and look at security updates as something that supplements Microsoft service packs.

It is true that Microsoft security updates are fairly comprehensive for the security vulnerabilities they address, and they are only released when they reach an appropriate level of quality.
But Microsoft service packs should be viewed as a broader vehicle, both in the scope of the updates they contain and the testing process they undertake.

A Microsoft service pack includes (where possible), all the security updates made available for that product before its release.

The service pack also contains other updates and improvements from the ongoing work of code maintenance that individual security updates may not contain, so it always offers the overall protections an IT Manager may need for their environment.

At Wanstor we believe an IT Manager's patch management strategy for Microsoft should first of all focus on service packs and then on security updates, rather than the other way around.

wanstor

Product Support Lifecycle

Directly related to the central role of service packs should be the role of the Microsoft Product Support Lifecycle in any patch management strategy.

Like all technology companies, Microsoft products follow a timeline of life cycle support. For several years now, Microsoft has worked to make this process as predictable and transparent as possible by developing and posting information about their Product Support Lifecycle (**www.microsoft.com/lifecycle**).

From a security perspective, one of the most important things a Product Support Lifecycle governs is the timeline for how long security updates for a particular product will be made publicly available. When a product is no longer publicly supported under the Product Support Lifecycle, Microsoft no longer publicly provides security updates for that product.

The Product Support Lifecycle is also relevant to the service pack principle which has already been discussed. Security update support for products is specific to particular service packs for that product.

This means that for as long as a product is publicly supported, security updates are made available only for those specific service packs of that product; updates are not made available for service packs of products that are no longer publicly supported.

By keeping up to date with service packs, IT Managers can make sure their IT environment is always in sync with the Product Support Lifecycle. Doing so means that an IT Manager should never be in a situation where security updates are released and they have no information about the vulnerable state of their environment because they are on an unsupported version of a Microsoft product.

At Wanstor, one tip we give to our customers is to integrate the timelines from the Product Support Lifecycle into their patch management strategy. This leaves them covered and aligned from a timeline perspective towards patch management.

Using the Severity Rating System as a starting point for risk

Microsoft security bulletins are there to make IT Managers aware that security updates are available for specific Microsoft products. Another goal of the bulletins is to help IT Managers with understanding issues in the security bulletin so they can perform a risk assessment of the issues in their IT environment in accordance with their businesses IT security policies.

Risk assessment is an important step in the practice of patch management because it helps to answer questions relevant to the prioritisation, testing, and deployment of security updates.

To help customers with risk assessment, Microsoft security bulletins use a Severity Rating System. With it, IT Managers can evaluate each issue and quantify the issue's impact objectively on a technical level using relevant criteria.

The Microsoft site for security bulletins can be found here:

https://technet.microsoft.com/en-us/security/gg309177.aspx

In the "Executive Summary" of each Security Bulletin, IT Managers will find a table that lists each vulnerability addressed in the bulletin and a severity rating for that vulnerability for each product which is affected. For bulletins that address multiple vulnerabilities in a product, a maximum severity for all vulnerabilities is provided. Additionally all security bulletins provide a summary so IT Managers can quickly and easily see what needs to be priortised.

The information in the security bulletins is intended to support the risk assessment processes and procedures that IT Managers have implemented as part of their patch management strategy.

Because the Severity Rating System evaluates the issue solely on technical grounds, it cannot account for specific aspects in each business environment.

At Wanstor We recommend IT Managers use the Severity Rating System as a starting point for their own risk assessment, then evaluate those elements specific to their business environment.

Determine applicability and priority through your own IT environmental knowledge

One of the pieces of technical information in the Security Bulletin relates to mitigating factors for each vulnerability addressed in that bulletin. Provided for each specific vulnerability in the "Vulnerability Details" section of the bulletin, the information about mitigating factors explains how the impact of the vulnerability may be lessened or mitigated and is important for IT Managers to assess the risk based on their knowledge of the IT environment they work within.

Mitigating factors are used in the Security Bulletins as part of the criteria in determining the severity under the Severity Rating System. E.g. A mitigating factor where a particular vulnerable component is disabled by default will result in a lower severity rating than if the component was enabled by default.

The main goal in explicitly calling out mitigating factors is to help IT Managers understand why an issue has been rated with a particular severity so they can undertake their own risk assessment process and have a starting point from which to work from.

Ultimately, IT Managers should use information about mitigating factors first to determine the applicability of an issue for their specific IT environment. If it is applicable, the IT Manager should then incorporate the information about mitigating factors into their risk assessment for prioritisation of the deployment of security updates.

Another important point to note is that information about mitigating factors is never meant to justify not deploying a security update. In examining mitigating factors, IT Managers should determine whether a vulnerability is applicable to their system or not. In the vast majority of cases Microsoft nearly always recommends that you apply the relevant security update.

At Wanstor we believe IT Managers should look at mitigating factors as data to answer the question of when to apply the security update, not if you should apply the security update.

MAKE SURE WORKAROUNDS ALIGN WITH DEPLOYMENTS

Make sure workarounds are aligned with deployments

As part of the process of investigating reports of vulnerabilities, Microsoft tries to identify workarounds that can protect against attempts to exploit the vulnerabilities being addressed by the security update. When Microsoft is able to identify viable workarounds to address a specific vulnerability, they make this information available in the Vulnerability Details section of the bulletin. When unable to identify a viable workaround, they generally make note of it instead.

The goal in providing workaround information for specific vulnerabilities is to give IT Managers an option they can use to protect their IT environments immediately, whilst security updates undergo appropriate testing before deployment. Just as mitigating factor information is never intended to justify not applying security updates, workaround information is provided as an interim measure until IT Managers can apply relevant security updates. This way, in patch management strategies, workarounds can be viewed as being closely tied to both risk assessment and deployment processes and procedures.

We recommend IT Managers consider implementing workarounds immediately for issues that are identified as posing a high risk to their environment in order to provide protections whilst they are deploying the updates. Issues for which there are no workarounds available will mean increased priority for deployments.

wanstor

Issues with Security Updates: Where are they?

At Wanstor a common question we receive from IT Managers in our customers after the release of security updates is, “Are there any known issues with the security update?”

The simple answer to this is Microsoft makes sure all security updates go through an extensive testing process and are only released when they meet an appropriate level of quality, but as part of the risk assessment process administrators often want to identify any known issues.

On rare occasions when an issue occurs after the application of a security update, that issue is documented in a Knowledge Base article by Microsoft’s Product Support Services.

It is important for IT Managers to know that any Knowledge Base article about a security update is also documented in the “Master Knowledge Base Article” for that Security Bulletin.

Each bulletin has a Master Knowledge Base Article associated with it that is referenced after the bulletin’s title. Additionally, the “Caveats” section in the summary is usually updated to highlight the inclusion of information in the Master Knowledge Base Article.

To see whether there are any known issues with a security update, look at the “Caveats” section of the bulletin. If there is no listing, take the Master Knowledge Base Article number from the security bulletin and view the Master Knowledge Base Article on the Microsoft Product Support Site (**http://support.microsoft.com**).

If there is no information there about known issues, it means that no issues have been identified with that security update.

Test updates before they are deployed

Testing security updates before deployment is an industry-recognised best practice. The correct testing of security updates allows IT Managers to understand the possible impact of the security update on their specific environment. This can be factored into understanding the potential risks before the deployment of the security update.

Just as the testing process should influence a risk assessment, the risk assessment should influence the testing process. Security updates that are identified as being particularly critical to an IT environment may merit a shortened testing cycle.

A security update that addresses an issue assessed as having low risk, but updates to critical systems instead may merit an extended testing phase to allow for broader and more thorough testing.

A common question we regularly come across at Wanstor is, “What should testing entail?” Unfortunately, there is no one universal answer for all businesses. The best answer we have to this question, is that it depends on your existing IT environment and the current business circumstances.

Generally the appropriate testing environment and procedures will depend on the production applications that are being run, the type and mixture of systems, and the resources that the IT department can afford to dedicate to testing. In general, though, Wanstor recommends a balanced cost vs resources approach dedicated to testing against the costs and resources potentially incurred by deploying an untested update in the existing IT environment.

Microsoft Product Support Services

An important piece of the testing process and procedures is what an IT Manager does when they think they have identified a possible issue with a security update in their environment. At Wanstor we strongly suggest that your procedures state that you get in touch with your Microsoft Services Partner before you do anything else.

Working with your Microsoft Services Partner is usually the most efficient way to identify genuine issues on those rare occasions when they do occur.

Only when your Microsoft Services Partner works with you directly are they able to gather the level of technical detail they need to understand what is actually happening. Your Microsoft Services Partner should be able to use that information to help address any genuine issues that are present in your IT environment.

It is also worth bearing in mind that if your Microsoft Services Partner cannot help you that Microsoft Product Services provides no-charge support for issues related to security updates. The best way to contact Microsoft directly is through their security support site.

wanstor

Methods and information for detection and deployment

Detection and deployment of security updates is a critical part of the patch management process. It's the application of the security update that addresses the vulnerability discussed in the Security Bulletin, and should always be the final step in a patch management process. It's also the piece of a patch management strategy that mostly falls on the systems management side.

This means that detection and deployment of security updates are sometimes handled by a group who do not read Microsoft Security Bulletins and are probably not aware of the specific information provided. This can lead to IT teams using methods of detection and deployment of security updates that have not been recommended in the Microsoft Security Bulletin.

Part of the process of building and releasing security updates is developing and verifying information for each security bulletin around detection and deployment. With this information, customers can identify systems the security updates apply to, and verify that they have been installed properly.

This information around detection and deployment is included in the Security Bulletin under the "Frequently asked questions (FAQ) related to this security update" and "Security Update Information" sections.

This critically important material represents the methods and information around detection and deployment that Microsoft has tested and verified to be accurate. Because other methods or information have not been tested, Microsoft cannot guarantee that they will be accurate or reliable.

Problems concerning detection and deployment directly affect the IT teams ability to successfully apply and manage security updates, so a critical piece of a patch management strategy needs to make sure only methods and information recommended in a bulletin for detection and deployment are used.

If the IT team are not currently using information from the security bulletins, they should immediately investigate implanting something like Windows Software Update Services (WSUS) or Systems Management Server to support detection and deployment.

If the IT team are currently using another patch management system, they should make sure it uses methods and information around detection and deployment included in the Microsoft Security Bulletin.

The Microsoft Security Bulletin is always the single source of truth

Any time there is a question about information related to a Microsoft Security update, the place an IT Manager should go for an answer is the Microsoft Security Bulletin that accompanies that security update. Information is entered into the bulletin after it has been verified for accuracy, so an IT Manager will know that information in a security bulletin is authoritative. Additionally, Microsoft will always put important information that is relevant to a security update in the Microsoft Security Bulletin, so an IT Manager can find information that is important about a security update.

Sometimes Microsoft gets new information that is relevant to a security update after it has been released. When Microsoft receives new information like this, they add that to the relevant bulletin. All changes to the security bulletins are documented at the bottom of the bulletin and are included in the date and the nature of the change. Anytime a bulletin is updated, the change is announced to the Security Notification Service, Comprehensive Edition (SNSCE). This list notifies all changes to security bulletins. The most important thing to take away from this section for IT Managers is Microsoft Security Bulletins are your single, authoritative source for the important information they need about Microsoft Security updates.

wanstor

Final Thoughts

By incorporating these principles of Microsoft patch management into a patch management strategy, IT Managers can help to make sure their processes and procedures are working in harmony with Microsoft.

In turn, it will mean a more efficient and effective approach to patch management, helping IT Managers better protect their IT systems.

For more information on Wanstor's patch management solutions, please call us on **0333 123 0360**, email us at **info@wanstor.com**, or visit us online at **www.wanstor.com**.

Wanstor | 124-126 Borough High Street | London | SE1 1LB |