wanstor

Patch Management

Service Description and Policy

Wanstor | 124 - 126 Borough High Street | London | SE1 1LB | 020 7592 7860 | info@wanstor.com

Service Outline

Wanstor provides managed patching services for our customers, it is essential for the security of these systems that they are regularly patched so as not to be vulnerable to known security issues for which fixes are available.

The purpose of this policy is to establish standard procedures for the identification of vulnerabilities, potential areas of functionality enhancements as well as the safe and timely installation of patches. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

Device Scope

This policy applies to all customer desktops and servers that run Microsoft, Mac OS and Linux operating systems and that are within the agreed scope for patching as part of Wanstor's managed patching service.

To ensure that an accurate collection of devices is onboarded, Wanstor recommend that an inventory scan of the network is performed during the initial onboarding phase.

Device Scope

The software within scope is defined as:

- Operating Systems listed on the "Supported OSs" tab*
- Microsoft Applications listed on the "Microsoft Applications" tab
- Third Party Applications listed on the "Third Party Applications" tab
- Anti-virus definitions listed on the "Support Anti-virus updates" tab

Please see: Microsoft Applications - Support by Desktop Central | ManageEngine for reference to the covered software versions.

All software (excluding VMware tools) listed above is in scope to be automatically patched according to the below Patch Types and schedules unless an exclusion is requested by the customer during the onboarding phase or via our change request process.

Patch Categorisation

Wanstor utilises ManageEngine's Severity rating, which references the Microsoft Severity rating[1], which in turn dictates the expected timeframe for the patch to be rolled out

Severity Rating

Rating	Description
Critical	A vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs without warnings or prompts. This could mean browsing to a web page or opening email. Microsoft recommends that customers apply Critical updates immediately.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. These scenarios include common use scenarios where client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered. Microsoft recommends that customers apply Important updates at the earliest opportunity.
Moderate	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations. Microsoft recommends that customers consider applying the security update.

[1] Microsoft Severity Rating System source: https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system

Low	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component. Microsoft recommends that customers evaluate whether to apply the security update to the affected systems.

Patch Rollout KPIs

The following KPIs apply to devices that are online and connected to the internet for at least 2 hours within the target period. Naturally if a device is offline during this period it will receive its updates once back online.

Zero-Day Vulnerability Security Patches

Where a vendor releases a patch outside of their usual patching cycle to address a publicly disclosed zero-day vulnerability, Wanstor will override the pilot group stage and release the patch to **all affected systems** within **72 hours.**. Pilot group devices will continue to have these updates pushed within **48 Hours.**

Critical or High Risk Security Patches

Wanstor will patch systems in scope within **14 days**, where the patch fixes a vulnerability with a severity that the product vendor describes as 'critical' or 'high risk'.*

*Only Redhat Linux machines can be patched with Security-only patches, this is also dependant on Redhat having issued a related bulletin ID for the vulnerability. For all other flavours of Linux, we can only a trigger an update of all modules and will be patched within **30 days** as per below.

Moderate or Low Risk Security Patches

Wanstor will patch systems in scope within **14 days**, where the patch fixes a vulnerability with a severity that the product vendor describes as 'moderate' or 'low risk'.

Non-Security Updates, Update Rollups and Server service packs

Wanstor will patch systems in scope within **30 days**, where the patch fixes a bug irrespective of the severity that the product vendor has assigned.

Feature Packs (Windows 10)

Windows 10 Feature Packs will not be rolled out automatically, these are considered to be project based rollouts, due to the additional testing that they will require.

Driver updates

Security updates for drivers on systems in scope will be patched within **14** or **30 days** according to the severity classifications described above.

Non-security, rollups or other types of driver patches will not be rolled out automatically.

Monitoring and Compliance

A compliance level refers to the percentage of computer devices that have been successfully patched or otherwise remediated such that they are no longer vulnerable. Wanstor will endeavour to achieve 100% compliance for Operating Systems under its management. Reporting of the current compliance level and suggested remediations can be made available via a monthly proactive service.

It is therefore critical that a customer's own policies require that machines to be patched are regularly powered on and that decommissioned machines are removed from active directory and also notified to the Wanstor service desk, for the attention of the Desktop Central team.

Scheduled Deployments

Patch Window

The patch schedule is determined by two factors: The window during the day (and which days) a patch can be deployed during and the group that the device resides in.

Desktop/End User Device patching window

By default this is set to:

- All day, every day (With the option for end users to postpone reboots up to 72 hours)

Server Patching Window

By default this is set to:

- All weeks, Sunday 00:00 – 06:00

These are our default practices, but may be varied by written request, please see the customizations section later in this document for more details.

Device groups

During the onboarding phase, Wanstor will work with you to categorize the devices into one of the following groups:

Pilot Group – Initial group of machines that will be patched, it would be beneficial to include at least one machine from each department/use case to act as the "canary in the coalmine" for new patches deployed.

- **Security updates** will be released to this group within **48 hours** of release by the vendor
- **Non-security updates** will be released to this group within **5 days** of release by the vendor

Standard Impact – Default grouping of machines that will be patched, unless specified, devices will be placed into this group by default

- **Security updates** will be released to this group after **5 days** of release by the vendor
- **Non-security updates** will be released to this group within **7 days** of release by the vendor

High Impact – Groups of machines that may be sensitive to disruption, where you would prefer that the patches have been in use in the rest of your organisation for a number of days first.

- **Security updates** will be released to this group after **7 days** of release by the vendor
- **Non-security updates** will be released to this group within **14 days** of release by the vendor

Customization

A customer may choose to customize any of the following settings; This customization must be requested in writing during the deployment phase or via Wanstor's change request process.

- Devices in scope
- Software in scope
- Severity rating of patches applied
- Deployment window for patches
- Reboot settings
- Notification settings
- Steps to take Pre/Post deployment of patches*

*Wanstor may apply an additional charge to "Baby Sit" installation of patches on complex systems; for example: Clusters where a failover, failback and application checks are required.

Policy

Roles & Access

Vulnerability assessment and system patching will only be performed by designated roles.

These roles are:

- Senior Systems Engineer
- Security Engineer
- Systems Engineer
- IT Infrastructure Manager

Vulnerability Information Sources

The following information sources will be taken as primary authorities on existing and new system vulnerabilities.

The patch repository used by Desktop Central is updated daily and the information can be found as following:

- Latest Security Patches: https://www.manageengine.com/products/desktop-central/patch-management/latest-security-updates.html
- Microsoft Security Bulletins: https://www.manageengine.com/products/desktop-central/patch-management/microsoft-security-bulletins.html
- Microsoft Products: https://www.manageengine.com/products/desktop-central/patch-management/microsoft-products-list.html
- 3rd Party Patches Supported: https://www.manageengine.com/products/desktop-central/patch-management/third-party-patches.html
- Mac Products: https://www.manageengine.com/products/desktop-central/patch-management/mac-patches.html

Patch Failure

In case of failure there will be an attempt to uninstall the patch or re-install the patch (depending on case), to remediate the issue. In the case of servers, if the remediation steps fail, a restore will be performed from backups.

To the extent permitted by law, Wanstor will not be liable for any loss and/or damage to data, caused by deploying a patch/update to any system or malfunctioning of the Desktop Central - ManageEngine software.

Changes and Exceptions to Patching Schedule

Exceptions to the patch management policy require formal documented approval from the Customer IT Infrastructure Manager. Any servers or workstations that do not comply with policy must have an approved exception on file.

The customer or the designated engineer is required to inform the Service Desk via a ticket about new servers created or decommissioned to take the steps required to include or remove them from the patching schedule. The ticket should be marked to the attention of the Desktop Central team.

Platform Maintenance

The Desktop Central service will require maintenance from time to time in order to upgrade, bug fix, patch the operating system and/or perform DB optimisations as and when required, usually out of hours. All of these will include downtime for the service itself, however, the customer will be notified in advanced as per the below explained maintenance advisories:

- Emergency maintenance/change: A system or process is broken or a problem has been discovered and is causing or has the potential to cause major disruption to the business and/or our customers if not dealt with as soon as possible (usually within 12 hours).
- Planned maintenance/change: A system or process is not working as efficiently as it should or a problem has been discovered and is causing or has the potential to cause minor disruption to the business and/or our customers if not dealt with (usually within 48 hours).

Glossary

Patch
A piece of software designed to fix problems (bug fixes, vulnerability fixes), or update (implement new features, etc.) to a computer program or its supporting data.

Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

Agent (Desktop Central Agent)
The Desktop Central agent is a lightweight software application that is installed on computers which are managed using Desktop Central. It helps to complete various tasks that are initiated in the Desktop Central server. For example, if you want to uninstall a software application from a computer in your network, you can make the required settings for this task in the Desktop Central server. The agent replicates these settings and ensures that the task is completed effectively.

The Agent is used for the patching process as well, it checks the Desktop Central server periodically for instructions related to tasks. The agent contacts the server when the following actions take place:

- User-specific Configurations:
  - Users log on
  - 90-minute refresh interval
- Computer-specific Configurations:
  - Computers are started
  - 90-minute refresh interval

Distribution Server
Where you have more than 100 computers at one of your locations, if each agent contacts the server to download the required patches, software binaries, etc., it will inevitably cause a bandwidth overhead. In such cases, we recommend to install a Distribution Server at that location. The distribution server periodically synchronizes

the patches and software binaries with the central server. The agents installed in the client computers will contact the Distribution Server to pull the tasks available for them and download the patch and software binaries from the distribution server.