# Windows Patching Overview

Monthly patching and maintenance of Windows servers is a crucial part of keeping server infrastructure secure and optimized. Regular patching helps protect the servers from vulnerabilities and ensures that they are up to date with the latest bug fixes and security patches.

By following these steps and implementing a structured approach to monthly patching and maintenance, the Organization can enhance the security and stability of Windows server environments. Regular patching helps safeguard infrastructure from potential threats and ensures that Business Key performance indicators (KPI's) are consistently met.

Below are a series of steps which the Celero Infrastructure Server Team follows during Windows patching.

**Establish a maintenance window:** Set a specific date and time each month for performing patching and maintenance activities. It's recommended to choose a time when server usage is low to minimize disruption to users and applications.

Currently the maintenance Window for all Oracle Cloud Infrastructure (OCI) servers is during 2nd weekend and 3rd Monday for (QA/NPD) environments. Whereas for Production environments 3rd and 4th Saturday’s following 2nd Tuesday of the month.

**Review patch releases:** Stay informed about the latest patches and updates released by Microsoft. Microsoft typically releases updates on the **Second Tuesday of each month**, known as **"Patch Tuesday."** Review the release notes and security bulletins associated with the patches to understand their significance and potential impact on environments.

**Test patches in a non-production environment:** Before deploying patches to Production servers, in the Oci environment, it's essential to test them in a QA/NPD/Sandbox environment. Set up a test environment that closely resembles a production environment and deploy the patches on a subset of non-production servers. This helps to ensure compatibility and identify any issues or conflicts with existing applications or configurations.

**Create a patching plan:** Based on the testing results, create a patching plan that outlines the order in which the servers will be patched. Consider any dependencies between servers, such as application or database servers that rely on specific components. Start with non-production servers and gradually move to production servers, ensuring proper testing and validation at each stage.

**Schedule server reboots:** Some patches may require a server reboot to complete the installation. Plan for server reboots during the maintenance window to minimize user impact. Coordinate with stakeholders and communicate the scheduled reboots in advance to avoid any user disruptions.

**Automate patch deployment:** Consider using automated patch deployment tools Azure Automation update management to streamline the patching process. These tools can help automate the download, approval, and deployment of patches across multiple compartments servers, saving time and reducing manual effort. Configure the tools to download patches in advance, so they are ready for deployment during the maintenance window.

**Monitor patch deployment:** Monitor the patch deployment progress to ensure that patches are successfully installed on all targeted servers. Use monitoring tools to track the installation status and identify any failed installations or issues that require attention. This allows you to take prompt remedial actions such as re-deploying failed patches or troubleshooting installation errors.

**Perform post-patching validation:** After the patching process is concluded, perform a post-patching validation to ensure the servers availability, test critical applications and services to verify their functionality and validate that the server configurations have not been adversely affected.

**Document patching activities:** Maintain a record of the patching activities performed on each server. Take a note of the patches installed, dates of installation, and any issues encountered during the process. This documentation will serve as a reference for future audits, troubleshooting, and tracking the overall patch management process.

**Stay informed:** Constantly stay informed about emerging security threats, vulnerabilities, and practices related to Windows Server patching. Regularly review Microsoft security bulletins, subscribe to security mailing lists, and follow trusted sources to ensure awareness of critical updates. This allows us to make quick adaptations to the patching strategy accordingly.