Automated Patch Management Policy

Objective

This Policy provides the processes and guidelines necessary to 1) maintain the integrity of network systems and data by applying the latest operating system and application security updates/patches in a timely manner, and 2) to establish a baseline methodology and time frame for patching and confirming patch-management compliance.

Desktops, laptops, servers, applications, and network devices represent access points to sensitive and confidential data as well as to technology resources and services. Ensuring that security updates and patches are distributed and implemented in a timely manner is essential towards mitigating malware, exploitation, and other threats

Scope

The processes addressed in this document affect all managed & unmanaged systems, including desktops, laptops, servers, network devices, and applications that connect to the network.

Prerequisite

This Policy should be read in conjunction with:

Information Technology Policies, including:

- IT SOP – Patch Management
- Change Management Policy

Responsibility

- Group Head Technology and Project Management
- Security Operations Centre
- Network Operation
- Application Developer
- Technical Assistance
- System Administrator

Policy

- SOC team will ensure the security patches are timely applied to all the servers, applications, and security devices available in JLI Production environment.
- Security operations team will notify to respective administrators & applications owners when new patches are available through patch manager (GFI Languard)
- SOC team will coordinate with system admins, network admins, DBAs, and application developers for patch analysis before applying the patches.
- SOC will deploy and install patches after a go head from respective DBA, system admins, network admins or application developers.
- SOC team will revert patches upon request from respective DBA, system admins, network admins or application developers if there are any issues found in the application after applying the patches.
- SOC team will maintain centralized repository of patches and will update the inventory upon patch installation or deinstallation.
- Patches which are not applied through SOC will be applied manually by respective administrator or developers as per patch management policy defined in IT SOP and repository will be updated.
- Manual Patching will be followed for (Core Application, Oracle Application Servers, Power BI Application, Web Server i.e., Xamp, Php, IWS, genesys and CRM machines)
- Oracle Databases, Hardware and network devices patch will be applied through manual process as per defined IT SOP.
- Client Java and JRE versions are excluded from the patch, because of obsoleted application versions.

Procedure

- Analysis – SOC will Review and analyze the patches and share the patch details that requires a review from Infrastructure team, Network Team, Application team, or Data Management team.
- Before patch application all stake holders, review will be taken by SOC.
- If patch is not recommended by Application owner or Infrastructure or network team or vendor, SOC will initiate the Patch Exception process.

Patch Exception Process:

- SOC Team along with respective application, network, infrastructure, or dba team owners will present the patch exception reasons to Group Head Technology & Project Management.
- Patch exception reasons must include the remedial actions or corrective measures and fall back plan along with the vendor recommendations.
- Group Head will analyze the exception and provide approval or rejection.
- Upon approval or rejection of the exception respective procedures will be followed.

Approval of Exception

If the approval is granted from Group head Technology & Project Management following actions will be taken by SOC/application owners or respective administrators.

- Apply the remedial actions – by administrator / application developer

- Record the risk acceptance reason in the centralized patch inventory – by SOC team

Rejection from Group Head

If approval is not granted from the Group head Technology & Project Management due to the high-risk vulnerabilities, following actions will be taken:

- Fallback plan must be revised
- Request SOC to apply the patch
- Test the server/application – if no issue recorded in 2 business weeks process will be marked as completed.
- If problem occurred during testing or with in 2 business week, post patch process will be initiated.

Post Patch Process

- Teams will jointly diagnose the problem and try to solve the problem along with available vendor of the application.
- If no solution is available in 3 business days or in defined RTO of the application, SOC team will initiate Patch Reversal Process.

Patch Reversal Process

- SOC will reverse the patch, once successfully reversed, SOC will update application developer / administrators to check the application.
- Upon confirmation of the test results from application developers or administrators process will either be mark as complete or old application / server backup will be restored after taking consent Group Head and other stake holders.
- After the restore make sure that application is up and running and patch inventory is updated

Patch Compliance Review

- Security Operation Centre will generate and review patch management & compliance reports at least monthly from the Centralized patch server.
- In reviewing the patch reports, server/network administrators & applications owner will identify un-patched machines that connect to the network and either patch or define an exception.
- The Security Operation Centre will conduct Missing patch scans of known critical systems at least monthly. Critical systems with un-patched vulnerabilities will be brought to the attention of the system/application owners(s) for mitigation.