

Patch Management Policy

1.1. Introduction

Purpose: This Patch Management Policy establishes the framework and directives for the systematic identification, evaluation, testing, deployment, and verification of software and system patches across World Bank's IT infrastructure. The primary goal is to mitigate information security risks arising from software vulnerabilities, ensure the stability and integrity of Bank systems, and maintain a robust security posture. Effective patch management involves the diligent application of updates to address known vulnerabilities, improve system functionality, and fix bugs, thereby reducing the overall cybersecurity risk exposure for the Bank.

Scope: This policy is applicable to all software components within World Bank's IT environment. This includes, but is not limited to, operating systems (server and client), enterprise applications (e.g., core banking, CRM, ERP), databases, middleware, firmware on network devices (routers, switches, firewalls), security appliances, and any other software or embedded systems owned, managed, or utilized by World Bank. It covers all environments, including production, development, testing, and disaster recovery.

Importance: The timely and effective application of patches is a critical operational and security requirement for World Bank. Unpatched vulnerabilities are a primary vector for cyberattacks, including ransomware and data breaches. Consistent patch management is essential for protecting against known exploits, meeting stringent regulatory and compliance obligations (such as those mandated by the FFIEC and PCI DSS), preventing financial losses, and safeguarding the Bank's reputation. Neglecting patch management can lead to severe consequences, including significant financial penalties and erosion of customer confidence.

1.2. Roles and Responsibilities

A collaborative approach is essential for effective patch management:

1.2.1. IT Operations Team: Responsible for the operational aspects of patch management, including the scheduled deployment of approved patches, conducting pre-deployment testing in non-production environments, verifying successful patch installation, and executing rollback procedures if necessary. They manage systems under their purview according to approved schedules and procedures.

1.2.2. Cybersecurity Team: Leads the vulnerability management aspect of patching. This includes identifying and tracking vulnerabilities through scanning and threat intelligence, performing risk assessments on identified vulnerabilities, prioritizing patches based on risk, providing oversight for the overall patching process, and coordinating emergency patch deployments in response to critical threats. They also define remediation timelines.

1.2.3. System Owners/Administrators: Accountable for ensuring that the systems and applications under their direct responsibility are patched in accordance with this policy. They collaborate with IT Operations for scheduling, participate in testing, and are responsible for validating the functionality and stability of their systems post-patching.

1.2.4. Change Advisory Board (CAB): The CAB is responsible for reviewing and approving patch deployments that are considered significant or high-risk. This typically includes patches that may require substantial system downtime, affect critical business services, or have a wide-ranging impact across the organization. The CAB ensures that changes are managed in a controlled manner.

1.3. Asset Inventory and Categorization

An accurate understanding of the IT environment is foundational to patch management.

1.3.1. Comprehensive Asset Inventory: World Bank will maintain a comprehensive, accurate, and regularly updated inventory of all hardware and software assets within its IT environment. This inventory must include details such as operating system versions, application names and versions, firmware versions for hardware devices, current patch levels, and asset ownership. An accurate asset inventory is the crucial first step in any patch management program, ensuring that no systems are overlooked.

1.3.2. System Criticality Classification: All systems and applications within the asset inventory will be classified based on their criticality to World Bank's business operations. A typical classification scheme includes: * **Critical:** Systems essential for core banking operations, customer-facing services, payment processing, or regulatory compliance. Downtime or compromise would have severe impact. (e.g., Core Banking System, SWIFT Gateway, Online Banking Platform). * **High:** Systems supporting important business functions, where downtime or compromise would cause significant disruption. (e.g., CRM, Loan Origination System). * **Medium:** Systems supporting general business operations, where downtime or compromise would cause moderate disruption. (e.g., Internal HR Portal, Intranet). * **Low:** Systems with minimal impact on core business operations if disrupted. (e.g., Non-critical departmental tools). This classification directly informs patch prioritization and testing rigor.

The effectiveness of patch management is shifting from a purely reactive, compliance-driven activity to a more proactive, integral component of risk-based vulnerability management. This evolution means that World Bank must not only apply patches but also deeply understand *why* specific patches are needed and *which* vulnerabilities should be addressed first, based on a quantitative assessment of actual risk to the Bank. This requires moving beyond simply checking boxes for audit purposes and instead, investing in robust vulnerability assessment tools and processes. These tools and processes should continuously feed information into the patch prioritization decision-making framework, ensuring that resources are focused on mitigating the vulnerabilities that pose the greatest and most immediate threat to the Bank's operations and data.

1.4. Vulnerability Identification and Assessment

Proactive identification and assessment of vulnerabilities are key to an effective patch management program.

1.4.1. Vulnerability Scanning: World Bank will conduct regular, automated vulnerability scans of all network-accessible assets. The frequency of these scans will be determined by system criticality: * Critical and High-risk systems: Scanned at least weekly. * Medium-risk systems: Scanned at least monthly. * Low-risk systems: Scanned at least quarterly. These scans will use Bank-approved vulnerability scanning tools to identify missing patches, misconfigurations, and other known vulnerabilities.

1.4.2. Monitoring Patch Sources: The Cybersecurity Team will continuously monitor various sources for information on new patch releases and vulnerability disclosures. These sources include: * Direct notifications and security advisories from software and hardware vendors (e.g., Microsoft, Oracle, Cisco, Adobe). * Security bulletins and alerts from reputable government agencies and industry organizations (e.g., CISA, NIST National Vulnerability Database - NVD). * Threat intelligence feeds and services that provide information on emerging threats and exploited vulnerabilities.

1.4.3. Vulnerability Analysis: Upon identification, each vulnerability will be analyzed by the Cybersecurity Team to determine its relevance to World Bank's environment. The analysis will include: * **Severity Assessment:** Primarily using the Common Vulnerability Scoring System (CVSS) to assign a numerical score (0-10) indicating severity. * **Exploitability Assessment:** Determining the likelihood of the vulnerability being exploited (e.g., availability of public exploit code, complexity of exploitation). * **Impact Assessment:** Evaluating the potential business impact if the vulnerability were to be exploited on specific Bank systems, considering data sensitivity and system criticality.

1.5. Patch Prioritization

Not all patches carry the same urgency. A risk-based approach ensures that critical vulnerabilities are addressed promptly.

1.5.1. Risk-Based Prioritization: Patches will be prioritized for deployment based on the overall risk they mitigate. This risk calculation considers: * The CVSS base score of the vulnerability. * The criticality of the affected system(s) (as per section 1.3.2). * The existence and prevalence of active exploits in the wild targeting the vulnerability. * The potential business impact (financial, reputational, operational, regulatory) if the vulnerability is exploited. * Compensating controls that may already be in place. This prioritization ensures that resources are directed towards the most significant threats first.

1.5.2. Remediation Timelines: World Bank establishes the following standard remediation timelines based on the assessed risk level of the vulnerability a patch addresses:

Table 1.A: Patch Risk Levels and Remediation Timelines

Risk Level	CVSS Score Range	Typical Characteristics	Standard Remediation Timeline	Emergency Patch Criteria
Critical	9.0 - 10.0	Easily exploitable remotely, often with no user interaction. High impact on confidentiality, integrity, or availability. Known public exploit may exist.	Within 7 to 14 calendar days	Active exploitation in the wild, specifically targeting the financial sector or World Bank.
High	7.0 - 8.9	Exploitable with some effort or specific conditions. Potential for significant impact on systems or data.	Within 30 calendar days	N/A (Handled by standard Critical timeline if exploitation becomes imminent).
Medium	4.0 - 6.9	More difficult to exploit, or impact is moderate. May require local access or specific user interaction.	Within 90 calendar days	N/A
Low	0.1 - 3.9	Very difficult to exploit, or impact is minimal. Often theoretical vulnerabilities or minor issues.	Within 180 calendar days or at next scheduled maintenance	N/A

Esporta in Fogli

This table provides objective criteria for classifying vulnerabilities and prioritizing patch deployment, ensuring consistency. It defines clear Service Level Agreements (SLAs) for remediation, crucial for operational planning and resource allocation. This structured, risk-based approach is often required by auditors and regulators, helps focus limited IT resources on the most significant threats first, sets clear expectations for teams regarding remediation speed, and directly contributes to reducing the Bank's overall cyber risk exposure.

1.5.3. Prioritization Meetings: The Cybersecurity Team and IT Operations Team will conduct regular meetings (e.g., weekly or bi-weekly) to review newly identified vulnerabilities, assess their risk in the context of World Bank's environment, and formally agree on patch deployment priorities and schedules, ensuring alignment with the established timelines.

An accurate and comprehensive asset inventory, as outlined in section 1.3, is an indispensable prerequisite for any effective patch management program. Without a clear and complete understanding of all hardware and software assets, their configurations, and their versions, it becomes impossible to ensure that all necessary patches are identified, prioritized, and applied correctly. This directly links the success of patch management to the robustness of secure configuration management practices (detailed in Document 7). If the asset inventory is incomplete or outdated, systems will invariably be missed during patching cycles, leaving them exposed to known vulnerabilities. Therefore, the success of this Patch Management Policy is fundamentally dependent on the quality of the asset management processes that are established and maintained, often as part of a broader configuration management discipline.

1.6. Patch Testing Procedures

While timely patching is crucial, deploying untested patches can introduce instability or new vulnerabilities.

1.6.1. Pre-Deployment Testing: All patches, particularly those intended for Critical or High-risk systems, must undergo thorough testing in a dedicated non-production environment (e.g., staging, User Acceptance Testing - UAT) before being deployed to the live production environment. This test environment should, as closely as possible, mirror the configuration of the production systems. Testing is a vital step to prevent patches from inadvertently causing system failures, application incompatibilities, or performance degradation. Rushing patches into production without adequate testing can be as detrimental as not patching at all.

1.6.2. Test Scope: The scope of patch testing should be comprehensive and include: * Verification of successful patch installation and removal (if applicable). * Assessment of system stability and performance post-patching. * Functional testing of core application features and business processes that rely on the patched system. * Verification of inter-system compatibility and integrations. * Security checks to ensure the patch does not introduce new vulnerabilities.

1.6.3. Rollback Plan: A documented rollback plan must be developed and available for every patch deployment, especially for production systems. This plan must detail the precise procedures required to revert the system(s) to their pre-patch state in the event that the patch causes critical issues or unforeseen negative impacts. The feasibility of the rollback plan should be assessed during the testing phase.

1.6.4. Test Group/Pilot Deployment: For patches that will be widely deployed across a large number of similar systems (e.g., operating system patches for employee workstations, common server OS patches), a pilot deployment to a small, representative subset of these systems in the production environment is highly recommended. This allows for monitoring in a live setting before a full-scale rollout and can help identify issues not caught in isolated test environments.

The failure to test patches adequately can lead to significant operational disruptions, which, in some cases, may be as damaging to the Bank as a security breach itself. A bad patch can break critical applications, corrupt data, or render systems unusable, leading to financial losses, customer dissatisfaction, and regulatory scrutiny. Therefore, a robust and well-executed testing phase is not a mere formality but a critical risk mitigation step. It ensures that the cure (the patch) is not worse than the disease (the vulnerability). This highlights the need for a balanced approach within patch management, where the urgency of security remediation is carefully weighed against the potential operational risks of deploying insufficiently tested changes.

1.7. Patch Deployment Schedule

Structured and predictable patch deployment minimizes disruption and maximizes efficiency.

1.7.1. Regular Patching Cycles: World Bank will establish and adhere to regular, predictable patching cycles. These cycles will be aligned with major vendor patch release schedules (e.g., "Patch Tuesday" for Microsoft products) and internal maintenance requirements. Common cycles may be monthly or quarterly for standard patching, depending on the system type and vendor. *Rationale:* Regular cycles allow for better planning, resource allocation, and communication.

1.7.2. Maintenance Windows: Patch deployments to production systems will be scheduled during pre-defined and formally communicated maintenance windows. These windows are typically established during off-peak hours, weekends, or other periods of low business activity to minimize disruption to critical banking operations and customer services. The duration and timing of maintenance windows will be agreed upon with business stakeholders. *Rationale:* Minimizes impact on business operations.

1.7.3. Automated Deployment Tools: To the extent feasible and secure, World Bank will utilize automated patch management and deployment tools. These tools can help ensure efficient, consistent, and widespread application of patches, reduce manual effort, and provide better tracking and reporting capabilities. *Rationale:* Improves efficiency, consistency, and scalability of patch deployment.

1.7.4. Communication: Relevant business units, system owners, and end-users (if directly impacted) will be notified in advance of scheduled patch deployments that may cause service interruptions or require system reboots. Communication will include the planned date, time, expected duration, and potential impact of the patching activity. *Rationale:* Manages expectations and allows users to plan accordingly.

1.8. Emergency Patching Procedures

For highly critical, actively exploited vulnerabilities, an accelerated process is required.

1.8.1. Definition of Emergency: An emergency patch is deemed necessary when a vulnerability is classified as Critical, is known to be actively exploited in the wild (particularly against the financial sector or similar organizations), poses an imminent and significant threat to World Bank's systems, data, or operations, and the risk of waiting for the next scheduled patching cycle is unacceptable. This often applies to "zero-day" vulnerabilities where a patch has just been released for an actively exploited flaw.

1.8.2. Expedited Process: In emergency situations, a predefined expedited process will be followed. This typically involves: * Immediate notification and convening of an emergency Change Advisory Board (eCAB) or designated senior IT and Cybersecurity management (e.g., CIO, CISO, Head of IT Operations, Head of Cybersecurity). * Rapid risk assessment and decision on immediate deployment. * Minimal or highly accelerated testing, focusing on basic stability and critical functionality, if time permits at all. In some cases, direct deployment to production may be authorized if the risk of not patching outweighs the risk of an untested patch. * Immediate deployment of the patch outside of standard maintenance windows.

Rationale: Allows for rapid response to severe threats, bypassing standard timelines when necessary.

1.8.3. Communication during Emergency: Rapid and clear communication is essential during emergency patching. The IT and Cybersecurity teams will disseminate information to relevant internal teams (e.g., SOC, Help Desk, application support) and, if necessary, to business stakeholders and potentially customers if significant service impact is anticipated. Business continuity plans may need to be referenced or activated.

1.8.4. Post-Emergency Review: All emergency patch deployments must be thoroughly documented, including the justification, approvals, actions taken, and any observed impact. A post-deployment review must be conducted within 24-48 hours to ensure system stability, confirm the vulnerability has been mitigated, and address any unforeseen issues. Lessons learned should be incorporated into future emergency response procedures.

1.9. Third-Party Software Patching

Patching requirements extend to all software, including applications provided by third parties.

1.9.1. Inventory of Third-Party Software: Maintain a comprehensive inventory of all third-party software applications used within World Bank, including version numbers and vendor details. This is part of the overall asset inventory (Section 1.3.1).

1.9.2. Vendor Monitoring: Actively monitor patch releases, security advisories, and vulnerability disclosures from all third-party software vendors whose products are used by the Bank. This may involve subscribing to vendor mailing lists, regularly checking support websites, or using software composition analysis tools.

1.9.3. Applicability Assessment: Assess the applicability and risk of vulnerabilities identified in third-party software using the same criteria (CVSS, criticality, exploitability, impact) as for operating systems or in-house developed applications. Prioritize and schedule patching of third-party software according to the remediation timelines defined in Section 1.5.2.

1.10. Unsupported Systems Management

Systems no longer supported by vendors pose a significant security risk.

1.10.1. Identification and Risk Assessment: Proactively identify all systems, operating systems, applications, and hardware components that are nearing or have passed their end-of-life (EOL) or end-of-support (EOS) dates as declared by the vendor. For each unsupported asset, conduct a formal risk assessment to understand the specific vulnerabilities and the potential impact on the Bank if these vulnerabilities are exploited.

1.10.2. Mitigation Plan: Develop a documented mitigation plan for all unsupported systems. The preferred approach is to upgrade or replace the unsupported asset with a supported version or alternative before the EOL/EOS date. If immediate replacement or upgrade is not feasible due to business constraints, the plan must include: * Implementation of compensating controls (e.g., network segmentation to isolate the system, enhanced

monitoring, application firewalls, restricted access). * A clear roadmap and timeline for eventual upgrade or replacement. * Formal risk acceptance documented and approved by senior management (e.g., CIO, CISO) and the relevant business owner, acknowledging the residual risk. This risk acceptance must be reviewed periodically.

1.11. Patch Verification and Validation

Ensuring patches are correctly applied and effective is crucial.

1.11.1. Post-Deployment Verification: After each patch deployment cycle, IT Operations must verify that the patches have been successfully installed on all targeted systems. Automated patch management tools often provide dashboards or reports for this purpose. Manual checks may be required for certain systems.

1.11.2. Functionality Testing: System owners and/or designated business users should conduct post-deployment functionality testing on critical applications and systems to ensure they are operating as expected and that the patch has not adversely affected core business processes.

1.11.3. Vulnerability Rescan: Following the deployment of security patches, the Cybersecurity Team should perform vulnerability rescans on the patched systems. This is to confirm that the targeted vulnerabilities have been successfully remediated and that the patch itself has not introduced new, unintended vulnerabilities.

1.12. Configuration Management Post-Patching

Patching can sometimes alter system configurations.

1.12.1. Configuration Review: Ensure that system configurations are reviewed and, if necessary, updated after patching to maintain alignment with World Bank's approved secure configuration baselines (as detailed in Document 7: Secure Configuration Rules).

1.12.2. Change Management: Any significant changes to system configurations resulting from or required by a patch deployment must follow World Bank's formal Change Management process. This ensures changes are documented, reviewed, and approved.

1.13. Documentation and Reporting

Comprehensive records are essential for compliance and operational oversight.

1.13.1. Patch Management Records: Maintain detailed and accurate records of all patch management activities. This documentation should include: * Vulnerability assessment reports and scan results. * Patch prioritization decisions and justifications. * Patch testing plans and results. * Deployment schedules, dates, and times. * Lists of systems patched and patch status (success/failure). * Verification and validation results (including rescan reports). * Any issues encountered and their resolution. * Rollback actions taken, if any.

1.13.2. Compliance Reporting: Generate regular reports for management review, internal audit, and external regulatory bodies to demonstrate patch compliance status. These reports

should show the overall patch levels across the environment, adherence to remediation timelines for different risk levels, and any outstanding exceptions. Automation should be leveraged for generating these reports where possible.

1.13.3. Audit Trails: Ensure that all patch management tools and associated processes provide clear, immutable audit trails of actions performed, including who initiated the action, what was done, and when it occurred. These logs must be protected and retained according to Bank policy.

Patch management is a continuous, cyclical process, not a one-time fix. It demands significant coordination across various teams including IT Operations, Cybersecurity, application owners, and often business units. For financial institutions like World Bank, robust patch management is not just a best practice but a cornerstone of regulatory compliance. Regulators expect to see evidence of a mature, well-documented, and consistently executed patch management program.

1.14. Exceptions Handling

Deviations from this policy must be managed formally.

1.14.1. Formal Exception Process: A formal, documented process must be followed for any requested exceptions to this Patch Management Policy. Examples might include delaying the deployment of a specific patch due to a critical incompatibility with an essential business application that cannot be immediately resolved, or a system that cannot be patched due to vendor restrictions.

1.14.2. Risk Assessment and Compensating Controls: All requests for exceptions must be accompanied by: * A thorough risk assessment detailing the vulnerabilities that will remain unpatched and the potential impact to the Bank. * A proposal for specific compensating controls to mitigate the risk posed by not applying the patch (e.g., enhanced monitoring, network isolation, stricter access controls). * Approval from the relevant System Owner, Head of IT Operations, and the CISO or designated Head of Cybersecurity.

1.14.3. Time-Bound Exceptions: Approved exceptions must be time-bound, with a specific review date (e.g., not exceeding 90 days). At the review date, the need for the exception must be re-evaluated. The goal should always be to remediate the underlying issue and apply the patch as soon as feasible. Exceptions should not be considered permanent solutions.

1.15. Policy Review and Updates

This Patch Management Policy will be reviewed at least annually by the IT Cybersecurity Team and the IT Operations Team, with input from other relevant stakeholders. The policy will be updated as necessary to: * Address new and evolving cybersecurity threats and vulnerability types. * Incorporate changes in technology and patch management tools. * Align with updated business requirements or organizational structures. * Reflect changes in regulatory

obligations or industry best practices. Approved updates will be communicated to all relevant personnel.