TECH THAT MATTERS

Elevaite365

Patch & Vulnerability Management Policy

Version 1.0

PURPOSE

This policy ensures that vulnerabilities, weaknesses, or exposures in IT and engineering resources or processes are identified, assessed, and remediated to prevent attacks that may lead to security or business risks. It outlines the technologies and procedures used by Elevaite365 (herein referred to as "Organization") to detect and remediate vulnerabilities, thereby maintaining maximum levels of security.

SCOPE

This policy applies to Policy Update Exercise Tenant and its employees and contractors. It encompasses the following areas:

1. **Desktop and Laptop Operating Environments:** Includes all employee workstations.
2. **Server Operating Environments:** Covers both on-premises and cloud-based servers.
3. **Network Devices and Equipment:** Routers, switches, firewalls, and other networking hardware are installed within the organization and in cloud environments.
4. **Code Repositories:** Applies to development, testing, and production environments where code is stored and managed.

DEFINITION

- **CVSS**: The Common Vulnerability Scoring System (CVSS) supplies a qualitative measure of severity for security vulnerabilities.
- **ISG**: Information Security Group
- **CISO**: Chief Information Security Officer – The executive overseeing the organization's information and data security strategies and implementations.
- **DevOps Head**: The leader responsible for the DevOps team, overseeing the integration of development and operations to ensure efficient and secure deployment processes.
- **Vulnerability**: A weakness in a system that can be exploited to compromise security, leading to unauthorized access, data breaches, or other malicious activities.
- **Patch**: A software update designed to fix vulnerabilities, improve functionality, or enhance security within an application or operating system.
- **Change Management:** Managing changes to IT systems to minimize disruptions, maintain security, and ensure that all changes are documented and approved.
- **Penetration Testing:** The practice of simulating cyberattacks against an organization's systems to identify vulnerabilities that could be potentially exploited.
- **Vulnerability Assessment is the** testing process used to identify and assign severity levels to as many security defects as possible within a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage.
- **Zero-Day Vulnerability:** A vulnerability unknown to those interested in mitigating the vulnerability (including the vendor of the target software).
- **Endpoint**: Any device that connects to the corporate network, including desktops, laptops, smartphones, and tablets.
- **Configuration Management**: The process of handling changes systematically so that a system maintains its integrity over time.
- **Remediation**: Correcting a system's vulnerability or weakness to prevent exploitation.

RESPONSIBILITIES

IT Head and DevOps Head

1. **Vulnerability Identification:** Periodically identify significant security vulnerabilities that may affect the Organization and its assets.
2. **Remediation Recommendations:** Recommend timelines for patch installation based on threat levels and organizational priorities.
3. **Monitoring:** Monitor the status of each vulnerability alert until its resolution, including any status changes and updates (e.g., exploit availability, patch availability).

4. **CVSS Management:** Update the Common Vulnerability Scoring System (CVSS) scores to reflect changes in vulnerability status.

Information Security Group (ISG)

1. **Policy Implementation:** Implement this policy with the IT and DevOps teams.
2. **Administrative Procedures:** Develop and maintain vulnerability scanning, assessment, and remediation procedures.
3. **Vendor Management:** Ensure that vulnerability scanning and assessment providers adhere to confidentiality and security requirements.
4. **Reporting:** Create annual vulnerability status reports to monitor the effectiveness of the policy.
5. **Training and Awareness:** Conduct training sessions to ensure all relevant personnel understand the policy and their roles in vulnerability management.

DevOps Team

1. **Patch Deployment:** Plan and deploy appropriate patches regularly following this policy.
2. **Configuration Management:** Ensure that all patches and fixes are tested in a test environment before being implemented in the production environment.
3. **Tracking and Documentation:** Track the progress of vulnerability remediation and document any exceptions approved by the DevOps Head.
4. **Tool Management:** Manage and maintain patch management tools and ensure they are updated and functioning correctly.

POLICY

VULNERABILITY IDENTIFICATION

The Organization identifies security vulnerabilities through the following methods:

1. **External Vulnerability Scans:** These are conducted at least annually on all public-facing IP addresses using an approved scanning vendor.
2. **External Network Penetration Tests:** Conducted at least annually.
3. **Post-Change Scanning:** External and internal vulnerability scanning is conducted after any significant infrastructure upgrade, application modification, or modification.
4. **Monitoring Industry Publications:** Monitor sources such as Security Focus, vendor security publications, etc., to identify zero-day vulnerabilities and other security issues.
5. **Virus Scanning Logs:** Conduct daily and real-time reviews of virus scanning logs.
6. **Security Logs Reviews:** Perform regular reviews of security issues reported in security logs.
7. **Audit Reviews:** Conduct reviews of security issues reported from internal and external audits.

VULNERABILITY MANAGEMENT

1. **Provider Agreements:** The vulnerability scanning and assessment provider must sign an agreement with the Organization before commencing work, including confidentiality provisions.
2. **Regular Scanning:** Providers will scan devices and systems under the scope and on the frequency set in the agreement, providing reports at least annually.
3. **Result Verification:** Upon receipt of a report, the Organization will verify the results to determine if there are false positives or perform penetration testing to validate exposures. Penetration testing will be done annually by an independent third-party vendor or more frequently if significant system changes occur.
4. **Remediation Planning:** Plan remediation by changing configurations, applying security patches, or updating code. Ensure the Change Management Policy and Procedure are followed, and changes are tested in a test environment before deployment.
5. **Mitigating Measures:** Implement mitigating measures. Any exceptions must be approved by the DevOps Head, with approvals and justifications recorded in the patch management tracker.

6. **Post-Remediation Scanning:** Once vulnerabilities are remediated, the provider will re-scan the system and provide a new report to ensure effective mitigation.
7. **Remediation Timeframes:** Based on risk assessment and prioritization using CVSS scores:

Vulnerability Rating	Description of the rating	Timeframe
Critical	Critical vulnerabilities provide attackers with remote root or administrator capabilities. Malicious users can compromise the entire host easily, leading to considerable asset damage.	5 business days or less, depending on the impact
High	High vulnerabilities allow attackers to gain privileged access (e.g., administrator or root) to the system. These vulnerabilities are often difficult to detect and exploit but can result in large asset damage.	10 business days or less, depending on the impact
Medium	Medium vulnerabilities allow attackers to gain non-privileged access or provide access that can be leveraged to gain administrator-level access. These issues are easy to detect and exploit but typically result in minor asset damage	30 business days or less, depending on the impact
Low	Low vulnerabilities provide minimal access or data sufficient to launch more informed attacks. They may indirectly lead to system access and are typically difficult to detect and exploit, resulting in minor asset damage.	Commercially reasonable time frame

1. **Tracking Progress:** The affected team will track the progress of vulnerability remediation.
2. **Annual Reporting:** The Engineering Guild will create vulnerability status reports annually to monitor the effectiveness of this policy.

PATCH MANAGEMENT

1. **Patch Tracking:** Implement an endpoint tool for patch management or maintain a tracker to monitor the progress of patch installations.
2. **Patch Categorization:** Categorize patches based on severity ratings (Critical, High, Medium, Low) per the vulnerability rating table above.
3. **Patch Validation:** Validate all vulnerabilities to isolate false positives.
4. **Testing Before Deployment:** All patches and fixes must be tested in a test environment before being implemented in the production environment.

Laptops / Desktops and Antivirus and Anti-Spamware / Malware Software Packages

1. **Critical and Security Patches:** Install the latest critical, security, and recommended patches for laptops, desktops, and other computing devices as soon as they become available.
2. **Patch Deployment:** Employees are responsible for deploying patches on their devices or systems on a priority basis.
3. **ISG Checks:** The ISG will periodically check and verify that all relevant patches are updated on devices and systems.
4. **Software Updates:** Update Microsoft Office and operating systems (e.g., Windows, Mac, Ubuntu) to the latest versions whenever available.
5. **Monthly Reviews:** Conduct random samplings of systems, desktops, and laptops monthly to review the effectiveness of patches. Record the results in the patch management tracker or on the patch management tool.
6. **Application Patches:** Deploy patches for applications, tools, and utilities used on laptops, desktops, and computing devices on a need basis.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan	Borhan,Linh	Borhan