Vulnerability Management Policy

Nexelus

Purpose

The purpose of this policy is to outline the requirements for (1) all product systems to be scanned for vulnerabilities at least annually, and (2) all vulnerability findings to be reported, tagged, and tracked to resolution in accordance with the SLAs defined herein. Records of findings must be retained for at least **1 Year**.

Roles and Responsibilities

The Network and Information Security Manager is responsible for establishing and maintain the policy. The acting Information Security Compliance Officer and Manager HR will ensure that all employees have reviewed and read the policy.

Policy

Information Systems Audit

The following guidelines will be observed for setting information systems audit controls:

- Audit requirements for access to systems and data should be agreed with appropriate management.
- Scope of technical audit tests should be agreed and controlled.
- Audit tests should be limited to read-only access to software and data.
- Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.
- Requirements for special or additional processing should be identified and agreed.
- Audit tests that could affect system availability should be run outside business hours.
- All access should be monitored and logged to produce a reference trail.

Vulnerability Scanning and Infrastructure Security Testing

The scanning and identification of Nexelus' system vulnerabilities is performed by:

- Automated Drata security agent installed on all employees' machines.
- **Endpoint Security Software**

Additionally, periodic security scans of Nexelus systems are done using a combination of external open-source and commercial vulnerability testing tools, including:

- **NMAP**

Penetration Testing

Penetration testing is performed regularly by either a certified penetration tester on Nexelus' security team or an independent third party.

Findings from a vulnerability scan and/or penetration test are analyzed by the Security Officer, together with IT and Engineering as needed, and reported through the process defined in the next section.

Security Findings Reporting, Tracking and Remediation

Nexelus follows a simple vulnerability tracking process using **Microsoft Dev Ops**. The records of findings are retained for 1 Year.

Reporting a Finding

- Upon identification of a vulnerability (including vulnerability in software, system, or process), a **Microsoft Dev Ops** ticket is created.
- The description of the Finding should include further details, without any confidential information, and a link to the source.
- The Finding will be given a priority level in **Microsoft Dev Ops**

Priority/Severity Ratings and Service Level Agreements

In an effort to quickly remediate security vulnerabilities, the following timelines have been put in place to address vulnerabilities:

Priority Level	SLA	Definition	Examples
Critical	**<CRITICAL SLA>**	Vulnerabilities that cause a privilege escalation on the platform from unprivileged to admin, allows remote code execution, financial theft, unauthorized access to/extraction of sensitive data, etc.	Vulnerabilities that result in Remote Code Execution such as Vertical Authentication bypass, SSRF, XXE, SQL Injection, User authentication bypass
High	**<HIGH SLA>**	Vulnerabilities that affect the security of the platform including the processes it supports.	Lateral authentication bypass, Stored XSS, some CSRF depending on impact
Medium	**<MEDIUM SLA>**	Vulnerabilities that affect multiple users, and require little or no user interaction to trigger	Reflective XSS, Direct object reference, URL Redirect, some CSRF depending on impact

Priority Level	SLA	Definition	Examples
Low	**<LOW SLA>**	Issues that affect singular users and require interaction or significant prerequisites (MitM) to trigger.	Common flaws, Debug information, Mixed Content

In the case a severity rating and/or priority level is updated after a vulnerability finding was originally created, the SLA is updated as follow:

- Priority upgrade: reset SLA from time of escalation
- Priority downgrade: SLA time remains the same from time of creation/identification of finding

Resolving a Finding

- The Finding should be assigned to the owner responsible for the system or software package.
- All findings should be addressed according to the established SLA.
- No software should be deployed to production with unresolved CRITICAL or HIGH findings, unless an Exception is in place (see below).
- A finding may be resolved by
    - providing a valid fix/mitigation
    - determining as a false positive
    - documenting an approved exception

Closing a Finding

- The assignee should provide a valid resolution (see above) and add a comment to the finding.
- The finding should be re-assigned to the Reporter or a member of the security team for validation.
- Upon validation, the finding can be marked as Done (closed) by the Reporter.
- Before the finding can be marked as closed by the reporter, the fix must be deployed to a development environment and have a targeted release date for deploying to production noted on the ticket.

Exceptions

- An Exception may be requested when a viable or direct fix to a vulnerability is not available. For example, a version of the package that contains the fix is not supported on the particular operating system in use.
- An alternative solution (a.k.a. compensating control) must be in place to address the original vulnerability such that the risk is mitigated. The compensating control may be technical or a process or a combination of both.
- An Exception must be opened in the form of a **Microsoft Dev Ops** ticket

- The Exception Issue must reference the original Finding by adding an Issue Link to the Finding issue.
- Each Exception must be reviewed and approved by the Security Officer and the impacted asset owner.