Vulnerability & Patch Management Process

v 1.2

Internal and Confidential

netradyne

Table of Contents

Document Control

Document Number	ISMS-050
Document Name	Vulnerability & Patch Management Process
Date of initial release	12-OCT-2021
Revision No	1.2
Information Classification	Internal
Prepared By	Sudhansu Kumar & Vijaykumar Dalal
Approved By	Saravanan Sankaran

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised By
1.0	12/OCT/2021	Patch Mgmt., Vulnerability Mgmt.	Vijay, Gautam, Sudhansu
1.0	28/OCT/2021	Revised roles & responsibilities for functional units, IT & InfoSec; Testing of Patches; Controlled Environment; Associating change tickets lifecycle	Sudhansu Kumar
1.1	16-APR-2023	Annual Revision	Sudhansu Kumar
1.2	09-JUN-2023	Changes incorporated in timelines and Exception	Sudhansu Kumar

Document Review/Approval

Date	Signatory Name	Organization/Signatory Title	Comments
27-12-2021	Saravanan Sankaran	Sr. Director, Infosec	
17-APR-2023	Saravanan Sankaran	Sr. Director, Infosec	
12-JUN-2023	Saravanan Sankaran	Sr. Director, Infosec	

Distribution of Final Document

Name	Organization/Title
All Organization	Netradyne

1 Purpose

This document establishes the vulnerability and patch management procedure for Netradyne. This policy defines requirements for the management of information security vulnerabilities and the notification, testing, and installation of security-related patches on devices connected to the Netradyne network. The purpose of this policy is to ensure that all Netradyne devices are proactively managed, identified vulnerabilities are remediated and patched with appropriate security updates. This document also provides guidelines to ensure that appropriate tools and methodologies are used to assess vulnerabilities in systems or applications, and to provide remediation adhered to prescribed timeline(s).

An appropriate security and vulnerability review shall be performed on cloud-based applications prior to deployment in a production and periodically while they are into operation. Result shall be reported to relevant stakeholders and identified vulnerabilities shall be remediated as per the prescribed timeline based on the level of risk.

Netradyne InfoSec Team will review, modify and amend this document from time to time for any changes in the process, policy & procedures. Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome. Any change in this document will be approved by InfoSec Head.

2 Scope

The scope of this document is applicable to all the Netradyne employees. The document is updated and developed as part of the day-to-day enterprise operations of the organisation. This policy applies to all the employees, contractors, vendors & guests of the organization who connects to the Netradyne network & systems.

3 Roles and Responsibilities for this document

Roles and responsibilities specific to this document are included below:

Role	***Responsibilities***
Owner	• Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. • Is the point of contact for the document. • Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process.
Reviewers/Stakeholders	Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality)
Approvers	The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead.
Document Release	Document Owner/team to work with repository administrator to make release version available.

4 Patch & Vulnerability Management Procedure

Patch and vulnerability management program is designed to proactively prevent the exploitation of system vulnerabilities that exist within Netradyne environment. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after an exploitation has occurred.

Patches are additional pieces of code developed to address problems/bugs in software. Patches enable additional functionality or address security flaws within a program. Vulnerabilities are flaws that can be exploited by a malicious entity to gain greater access or privileges than it is authorized to have in Netradyne environment. Not all vulnerabilities have related patches; thus, system owner/administrators must not only be aware of applicable vulnerabilities and available patches, but also other methods of remediation (e.g., device or network configuration changes, employee training) that limit the exposure of systems to vulnerabilities.

4.1 Roles & Responsibilities for Patch & Vulnerability Management Procedure

4.1.1 IT Director

- Review and provide consultation to any changes to the Patch Management policies & procedures for the organization
- Accountable for ensuring that IT System Inventory is up-to-date, and IT assets are patched and free from any vulnerability

4.1.2 InfoSec

- Review and approve the changes to the Patch Management policies & procedures for the organization
- Validate Patch Deployment/Vulnerability Remediation through System Vulnerability Scanning
- Periodic compliance checks with the Vulnerability and Patch management procedure & Timelines
- Monthly Reporting on Vulnerability & Patch management compliance to Management and Functional Owners
- Define Exception Process for Vulnerability & Patch Management. For any exception on valid reasons, approvals are needed from System Owner (First Level) and InfoSec Head (Second Level)
- InfoSec team will review each exception in consultation with IT team/Respective Functional Team

4.1.3 IT Team

- **Create a system inventory**- IT Team should use existing inventories of the organization's IT resources to determine which hardware equipment, operating systems, and software applications are used within the organization. They should also maintain a manual inventory of IT resources which are not captured in the existing inventories
- **Scope the IT team responsibility as per the Identified system inventory**, where assets are managed by IT Team, and they are performing end to end system management
- **Monitor for Vulnerabilities, Patches & Threats on Organization's IT resources**- IT Team is responsible for monitoring security sources for vulnerability/Patch announcements, patch, and non-patch remediations, and emerging threats that correspond to the software within the **IT managed resources**.
- **Prioritize Vulnerability Remediation and Patching-** Assess the criticality of vulnerabilities and patches in Netradyne environment and prioritize as per identified classifications
- **Download Remediation Packages/Patches from trusted source in secure manner**

- **Conduct Testing of Remediations/Patches** in test environment as per change management process
- **Deploy Vulnerability Remediations/Patches in controlled environment using the same change ticket** after successful test result- IT Team should deploy patches automatically within the IT's system inventory using Centralize Patch Management Tool
- **Prepare Pre-Patch and Post-Patch Reports; Update Change record with** subsequent action(s) from test to successful deployment.

4.1.4 Functional Owner (e.g., DevOps, Device & Analytics etc.)

Any system which does not fall under IT Team management and end to end managed by either Device Team, DevOps Team, Analytics Team or any other functional unit; the responsibility of Patch/Vulnerability discovery, Download the same from trusted source, assess the severity of patches/vulnerability, change record creation and managing its lifecycle, test and deploy the patches/remediation to system is respective team's responsibilities.

- Create respective asset inventory
- Monitor for vulnerabilities, remediations for their assets
- Assess and prioritize the patches/vulnerability remediation in Netradyne environment
- Conduct testing of patches and ensure that patches & remediations are not hindering normal application/system behaviour and business processes will run as usual. In case of non-feasibility follow the Patch/Vulnerability remediation exception process as described in section 6.

4.2 Patch Management Procedure

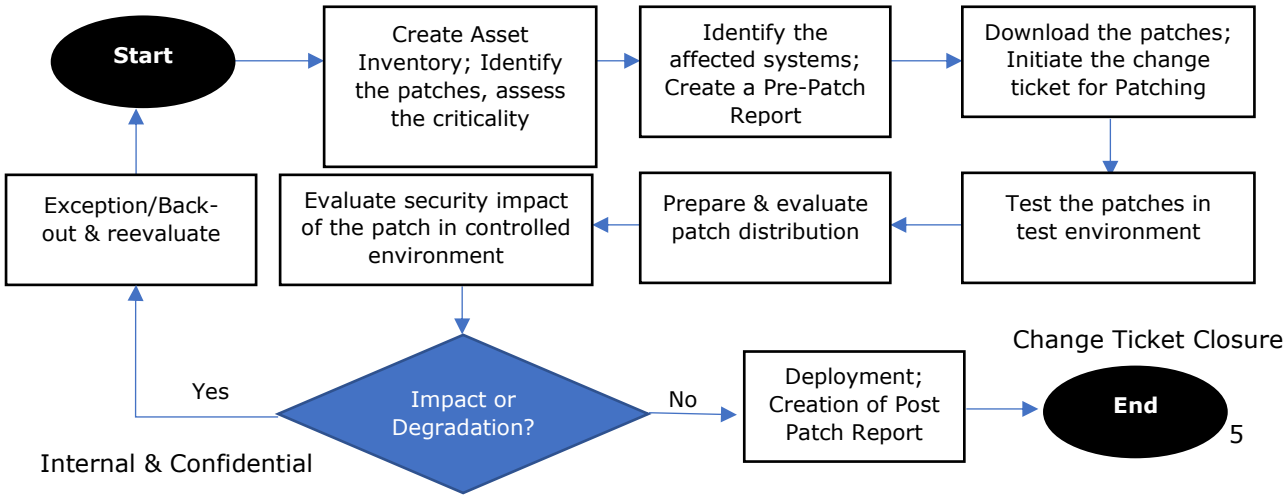
There are a high number of systems and applications in use at NETRADYNE and ensuring they are fully patched and secured in a controlled manner is a priority. This includes all aspects of infrastructure, applications, and any other hardware and software.

In its corporate and development environments, NETRADYNE currently use packaging and configuration management system to ensure all systems receive the latest security and functional software patches and fixes as ready.

In the production environment, NETRADYNE works to ensure patches are applied in a controlled and non-disruptive manner using a group of tools. **Critical patches** are immediately evaluated and deployed immediately or **within 5 days**. High severity patches should also be applied immediately or within 30 business days, **Medium and Low severity patches** are reviewed as part of the internal audit process and generally **deployed within 3 and 12 months respectively,** depending on relevance and severity.

All patches must deploy in adherence to NETRADYNE's change management policy. **This includes initiate a change ticket or get and umbrella approval for regular periodic patches (e.g., Microsoft released OS patches comes every month on 2nd Tuesday), download & test patches before deployment to production in controlled environment.**

The flow below depicts high-level patch management process followed in Netradyne for respective System Owner/Administrator:



Procedure Steps: The following phases must be followed to comply with this procedure:

4.2.1 General

- All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches.
- System components and devices attached to the Netradyne network shall be regularly maintained by applying critical security patches within a month after the patches are released by the vendor.
- Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

4.2.2 System, Utility, Application & Device Firmware Patching

- A periodic schedule shall be developed for security patching of all Netradyne systems and devices. Patching shall include the updates to all operating systems, Firmware's, productive software's, third party applications etc. either by Netradyne IT department or respective function unit which manages the affected resource(s). We should classify and remediate the patches with respect to Netradyne's live environment e.g. SaaS Hosting, Netradyne Products used by our partners, SaaS products used by Netradyne, Netradyne Internal System Managed by IT Team etc.
- Most vendors have automated patching procedures for their individual applications. Approved Patch Deployment Tool(s) shall support the patching process across the many different platforms and devices that Netradyne supports.
- The regular application of critical security patches is reviewed as part of normal change management and audit procedures by Netradyne

4.2.3 Stages in OS Patch Management-Managed by IT Team

Patch Deployment phases should align with the steps described in Sub-Sections 4.1.3 & 4.1.4. OS Patching is performed with the help of approved Patch Deployment tool. The Central Patch Repository is a portal in the Zoho Corp. site, which hosts the latest vulnerability database that has been published after a thorough analysis. The users of Desktop Central application are granted access to the Central Patch repository, to periodically download the vulnerability database. It scans the systems in the enterprise network, checks for missing and available patches against the comprehensive vulnerability database, downloads and deploys missing patches and service packs, generates reports to effectively manage the patch management process in the enterprise.

Patch Management using Desktop Central is a simple two-stage process:

4.2.3.1 Patch Assessment or Scanning:

- Desktop Central periodically scans the systems in your network to assess the patch needs. Using a comprehensive database consolidated from Microsoft's and others, the scanning mechanism checks for the existence and state of the patches by performing file version checks, registry checks and checksums. The vulnerability database is periodically updated with the latest information on patches, from the Central Patch Repository. The scanning logic automatically determines which updates are needed on each client system, considering the operating system, application, and update dependencies.
- On successful completion of an assessment, the results of each assessment are returned and stored in the server database. The scan results can be viewed from the web-console.

4.2.3.2 Patch download and deployment:

- On selecting the patches to be deployed, you can a trigger a download or a deploy request. At first the selected patches are downloaded from the internet and stored in a particular location in the Desktop Central server. Then they are pushed to the target machines remotely, after which they are installed sequentially. Patch deployment should always be done in controlled environment in order to revert to original state, in case of any anomaly or peculiar system behaviour.

4.2.3.3 Patch Verification

Implemented patches need to be verified on periodic basis by InfoSec. Pre and Post patch reports need to be created and maintained by IT Team. Patch deployments need to be tracked for closure.

4.3 Vulnerability Management Procedure

Vulnerability remediation phases shall align with the steps described in Sub-Sections 4.1.3 & 4.1.4.

Procedure Steps: The following phases should be followed to comply with this procedure:

4.3.1 Vulnerability Identification Phase

Vulnerability scanners, risk assessment, code reviews and penetration testing shall be used to discover the security weakness/vulnerabilities in the resources. InfoSec are responsible for ensuring all resources are scanned periodically, reviewing the results of the scan, and determining, what, if any, additional mitigations or remediations activities are required to be implemented, based on the vulnerability's risk level described in Vulnerability Classification.

InfoSec will also be responsible for Risk Assessments and Penetration testing. Conducting DevOps related vulnerability identification methods (Code reviews, Static code analysis etc.) would be DevOps/Cloud Team responsibilities.

Vulnerability scans shall be conducted periodically on all Netradyne assets to detect new and non-remediated vulnerabilities. Relevant team(s) analyse and remediate "Critical", "High", "Medium" and "Low" rated vulnerabilities as per the prescribed timeline(s) mentioned in section 4.3.3.5 or shall have received documented and approved exceptions from the Infosec.

4.3.2 Vulnerability Classification Phase

Discovered vulnerabilities in the resources are reviewed, prioritized, and assessed using results from technical and risk reports. The following vulnerability risk classifications describe severity levels that may be assigned to an identified vulnerability with an attempt to consolidate terminology used as it relates to this standard. **However, the Assessor should consider the Netradyne Security Environment before determining the final severity**.

Sources for cybersecurity vulnerabilities information, CVSS scores, and related risks and exposure include: the National Vulnerability Database, which can be found at https://nvd.nist.gov/vuln-metrics/cvss and, the Common Vulnerability Exposure Database, located at https://cve.mitre.org/.

4.3.2.1 Critical Risk Vulnerabilities:

Flaws could be easily exploited by a direct or indirect attack at any point of time and will create decisive or significant effect. Netradyne existing security controls are not sufficient to prevent/detect the exploit.

4.3.2.2 High Risk vulnerabilities:

These types of vulnerabilities allow local users to gain privileges, allow unauthenticated, remote users to execute arbitrary code, or allow remote users to cause a DoS. Netradyne existing security controls are not sufficient to prevent/detect the exploit.

4.3.2.3 Medium Risk Vulnerabilities:

This is classification is given to the flaws that may be more difficult to exploit but could still lead to compromise under certain circumstances. These are the types of vulnerabilities that have a critical or important impact but are less easily exploited based on technical evaluation of the flaw, or effect require an unlikely configuration.

4.3.2.4 Low Risk Vulnerabilities:

These are types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would cause either no adverse effect or result in only very minimal adverse consequences.

4.3.3 Vulnerability Mitigation and Remediation Phase:

Below are the vulnerability mitigation states and phases:

4.3.3.1 False Negatives, False Positives, and Not Applicable Results False Negatives:

All Functional Units are responsible for ensuring vulnerability scans are not hindered due to inadequate access to the resources being scanned. This will cause inaccurate and/or incomplete results to be produced. In many cases, credentialed scans should be utilized to ensure that scans analyse the entire system and produce accurate and comprehensive results. Without required access levels, scan results may produce 'false negative' results which provided an inaccurate picture of the security posture of the system being scanned.

4.3.3.2 False Positives or Not Applicable Results:

If the identified vulnerability is believed to be a false positive, or is otherwise believed not applicable, the following information is required to be concisely documented and made available for Infosec review.

- The affected system(s) and vulnerability.
- The plugin/service/software causing the false positive.
- Information/processes used to confirm the vulnerability is, in fact, a false positive or not applicable.

4.3.3.3 Mitigation and Remediation Requirements:

After confirming the vulnerability scan results that are applicable to their resources, units are responsible for addressing the risks presented by such vulnerabilities, through implementation of required vulnerability risk mitigation and remediation strategies.

Where possible, units are required to permanently resolve the risks associated with the vulnerability through implementation of permanent fixes that will usually include installation of vendor security patches, firmware updates and/or configuration changes. Permanent fixes also may require changes to functional unit-specific policies and procedures. All changes should be documented and made available for Infosec review upon request, as previously discussed.

If a vendor security patch or configuration change is not available to permanently resolve the risk associated with the vulnerability, functional units will be required to develop and implement compensating controls. The controls are required to mitigate the risks of the vulnerability and shall be consistently implemented until a permanent remediation is implemented.

4.3.3.4 Remediation Strategies:

We should classify, group and remediate the vulnerabilities with respect to Netradyne's live environment e.g. SaaS Hosting, Netradyne Products used by our partners, SaaS products used by Netradyne, Netradyne Internal System Managed by IT Team etc. Remediation shall be performed by associated functional units as per the above identified classification(s). Few examples of remediation steps are listed below:

- Patching the software or service and developing a continuous remediation process.
- Harden the devices/appliances adequately
- Removing the software or services that are not needed, if possible.
- Implement configuration changes using security features within the resources of DevOps to further reduce the attack plane.
- Remediation for each identified vulnerability shall be tracked for closure by leveraging respective tools. Any non-compliance must be reported to leadership.

4.3.3.5 Mitigation and Remediation Timeline Requirements:

Critical Risk Vulnerabilities: Mitigation and/or remediation is required to address all critical risk vulnerabilities on all affected systems immediately or within **5** days.

High Risk Vulnerabilities: Mitigation and/or remediation is required to address all high-risk vulnerabilities on all affected systems immediately or within **30** days.

Medium Risk Vulnerabilities: Mitigation and/or remediation is required to address all medium risk vulnerabilities on all affected systems within **90** business days.

Low Risk Vulnerabilities: Mitigation and/or remediation is required to address all low-risk vulnerabilities on all affected systems within **12** Months.

Any deviation in remediation/deployment timeline shall be approved as an exception with proper justifications and recorded in Netradyne Risk Register.

5 Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

6 Exception

Exception to this procedure must be approved through the Netradyne Exception Management Process. Any deviation in remediation/deployment timeline shall be approved as an exception with proper justifications and recorded in Netradyne Risk Register.

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate business needs or Mitigation is practically not possible within the prescribed duration To request a security exception, contact the InfoSec team. Below are the examples of exceptions:

- Patching on Production systems like GPU machines hosted in our data centre may require complex testing and installation procedures

- Deviations from normal patch schedules shall require authorization from IT & InfoSec Head
- Inability to remediate a vulnerability due to lack of solution
- Patch/Remediation are not feasible with application and business requirements

For any exception in patch deployment/vulnerability remediation on valid reasons, approvals are needed from System Owner (First Level) and InfoSec Head (Second Level)

7 Terms/Acronyms

Term/Acronym	Definition
Resources	include computing, networking, communications, application, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.
Production Environment	This is commonly used for any live environment in Netradyne e.g. SaaS Hosting, Netradyne Products used by our partners, SaaS products used by Netradyne, Netradyne Internal System Managed by IT Team etc. *(In future Patch & Vulnerability Management Procedure document will be more refined and dedicated procedures will be added to different type of production environment(s) as mentioned above.)*
Patch	is a software update comprised of code inserted (i.e., patched) into an executable program code. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited, to the following: • Upgrading software • Fixing a software bug • Installing new drivers • Addressing security vulnerabilities • Addressing software stability issues
Remediation	is an effort that resolves or mitigates a discovered vulnerability.
Vulnerability	is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Vulnerability management	is the practice of identifying, classifying, remediating, and mitigating vulnerabilities.
DL	Distribution List
ND	Netradyne

8 References

8.1 Templates

<List of (or Links to) associated templates>

8.2 Policies

<List of (or Links to) associated corporate level policies>

8.3 Netradyne Information Security Policy & Procedure.pdf

8.4 Process/Procedures

Netradyne Information Security Exception Process.pdf

8.5 NetradyneSecurityIncidentResponsePlan.pdf Standards

<List of (or Links to) related Netradyne Standards>

8.6 Miscellaneous

<List of (or Links to) any relevant documentation not covered in the list above>

9 Appendix A: Document RACI Matrix

Role/Activity	Document Owner/InfoSec Head	Document Contributor	ND Leadership	Functional Area Team	InfoSec Team	All ND Member(s)
Ensure document is kept current	A	R	I, C	R, C	C	I
Ensure stakeholders are kept informed	A	R	-	R	C	-
Ensure document contains all relevant information	A	R	I, C	R, C	C	I
Ensure document adheres to document governance policy	A, R	R	I	R, C	R, C	I
Provide SME advice	I, R	A, R	I	R, C	I, C	I
Gathering and adding document contents	I	A, R	I, C	R, C	C	I
Document Approval	A	R	I, R	I	I, R	I

Key

R	Responsible
A	Accountable
C	Consulted
I	Informed