


Vulnerability and Patch Management Procedure

Ncell

Approved Date:- 15/08/2019

	Ncell	Classification: Internal
	Vulnerability and Patch Management Procedure	Owner: CIO/Head of IT
		Effective Date: 15 th August, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Procedure Name DOCID: PR-IT-IS-06

Copyright © Ncell. All rights reserved.

No part of this document may be reproduced or transferred in any form or by any means without prior permission in writing from Ncell.

These trademarks are the intellectual property of Ncell and are protected by applicable legislation.

All other products or company names are used for reference only and may be proprietary to their respective hold

	Ncell	Classification: Internal
	Vulnerability and Patch Management Procedure	Owner: CIO/Head of IT
		Effective Date: 15 th August, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Document Control

i. Document Identification

Document Title and Version:	PR-IT-IS-06 Vulnerability and Patch Management Procedure
Effective Date:	15 th August, 2019
Document Author:	Information Security Team
Owner:	Information Security Team

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor's (If Required)


iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO

CIO/Head Of IT

	Ncell	Classification: Internal
	Vulnerability and Patch Management Procedure	Owner: CIO/Head of IT
		Effective Date: 15 th August, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

v. Revision History

Rev	Date	Author	Description	Approved By	Initiated Date
0	15-08-2019	Information Security Team	Initial document	CEO	15-08-2019
1	15-09-2019	Information Security Team	Revised – Formatting Changes	CEO	15-09-2019
2	15-05-2020	Information Security Team	Changes made for Kernel closure cycle. Clarity on SLA Remediation Process	Vishal Mani Upadhyay	15-05-2020
3	22-10-2021	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	19-12-2021
4	19-12-2021	Tarani Prasad Chaudhary	Review- Formatting	Andy Chong	20-12-2019
5	23-08-2023	Information Security Team	2. Review changed from annually to once in every two years 5.4. viii: updated Ncell by functional teams. Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
6	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
7	30-04-2024	Information Security Team	Re-branding	CIO/Head of IT	

Ncell	Ncell	Classification: Internal
	Vulnerability and Patch Management Procedure	Owner: CIO/Head of IT
		Effective Date: 15 th August, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Table of Contents

Document Control	2
1. Purpose	5
2. Review and Updating	5
3. Scope	5
4. Roles and Responsibilities	5
4.1 Information Security Team	5
4.2 System/Services Owners/ Unit Heads & Above	5
5. Vulnerability and Patch Management Lifecycle	5
5.1 Vulnerability Planning and Identification	5
5.2 Vulnerability Scanning	6
5.3 Vulnerability Reporting	6
5.4 Vulnerability Remediation	7
5.5 Patch Management Cycle	7
5.6 Independent Reviews	7
5.7 Deployment of New Systems	8
6. Management Reporting	8
7. Governance and Compliance	8
8. Associated Documents	8

Ncell	Ncell	Classification: Internal
	Vulnerability and Patch Management Procedure	Owner: CIO/Head of IT
		Effective Date: 15 th August, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

1. Purpose

The purpose of this policy is to establish a single, consistent approach to managing security vulnerabilities through patch and configuration management at Ncell. This approach includes specific timeframes for mitigating risk associated with vulnerabilities.

2. Review and Updating

This procedure shall be reviewed once in every two years or whenever significant changes occur in the organization.

3. Scope

This document is applicable to all Ncell applications and supporting infrastructure.

4. Roles and Responsibilities

4.1 Information Security Team

The Information Security Team is responsible for:

- Planning and conducting periodic assessments of applications and infrastructure components to identify vulnerabilities,
- Tracking the identified vulnerabilities, the impacted technology resources and the analysis of the risk associated,
- maintaining and protecting the VAPT (Vulnerability Assessment and Penetration Testing) reports and records,
- Managing communication and training for the Vulnerability Management program, processes, procedures, tools, and resources,
- Reporting status of the Vulnerability Management program efforts and cases of non-compliance to Head of IT periodically, and
- Ensuring that adequate resources with appropriate skillsets are in place to ensure testing and reviews as scheduled.

4.2 System/Services Owners/ Unit Heads & Above

The system owners are responsible for:

- Preparation of corrective action plan for identified vulnerabilities,
- Remediation of vulnerabilities within defined time period,
- Maintaining the patch management records,
- Sharing the remediation report with the Information Security Team, and
- Sharing the updated asset inventory with the Information Security Team.

5. Vulnerability and Patch Management Lifecycle

5.1 Vulnerability Planning and Identification

The following controls should be adhered to:

- An inventory of IT Assets that processes and/or stores NCELL data. The asset inventory must provide information regarding the asset type, hardware type (e.g., hardware, software, and application), service/risk owners, vendor information, pre-production vs. production status, relative versioning and patch levels, and IT Asset Custodians responsible for each asset shall be maintained.
- IT Asset Custodians and third-party suppliers with equipment on NCELL premises must establish a Security Maintenance Window in which to conduct operational security activities such as patching.
- IT Asset Custodians and third-party suppliers with equipment on NCELL premises must clearly communicate and make known to Ncell stakeholder groups, the time and duration of the dedicated Security Maintenance Window.
- Ncell shall ensure that the Asset inventory configuration and change control procedures are coordinated with current asset inventories and updated accordingly.

Ncell	Ncell	Classification: Internal
	Vulnerability and Patch Management Procedure	Owner: CIO/Head of IT
		Effective Date: 15 th August, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- v. Ncell shall ensure that vulnerabilities that could be used to compromise its assets are identified through periodic testing or reviews. The risk ratings shall be assigned to vulnerabilities identified taking into consideration the risk score and/or the classification and criticality of the affected system.
- vi. Where possible, automatic notification of vulnerabilities from external sources shall be enabled.
- vii. Where automatic notifications are not available, Ncell should subscribe to industry and vendor notifications and vulnerabilities advisories.
- viii. Multiple sources of information shall be used to monitor for vulnerability notices for each technology resource type. Sources may include:
 - ix. Vendor Web sites and mailing lists,
 - a. Third-party Web sites,
 - b. Third-party mailing lists and newsgroups,
 - c. Vulnerability scanners,
 - d. Vulnerability databases,
 - e. Enterprise patch management tools, and
 - f. Other notification tools.
- x. Vulnerability notifications received or acquired for each technology resource shall be distributed to resource owners and appropriate information security personnel.

5.2 Vulnerability Scanning

The following controls should be adhered to:

- i. Ncell shall perform periodic scanning of all information technology resources for known vulnerabilities. Scanning will include web application vulnerabilities, database configuration vulnerabilities, and all other technology resource types and vendors.
- ii. Vulnerability scanning shall be performed using commercially available tools and technologies and a current set of available vulnerability policies or signatures.
- iii. Vulnerability assessments shall be performed at least monthly for crown jewels and infrastructure components and annually for non-critical applications and infrastructure components to identify any new or existing vulnerabilities.
- iv. Vulnerability scanning shall be performed on all new technology resources prior to the deployment of the resources on Ncell's program wide networks and during major configuration or system updates.
- v. External vulnerability scans will be performed:
 - a. From outside the Ncell's program wide network perimeter at least on an annual basis to identify potential vulnerabilities that could be exploited by external threats.
 - b. On a quarterly basis against external ports to track externally available services and compared to a listing of approved service ports to identify potentially new and unauthorized services.

5.3 Vulnerability Reporting

The following controls should be adhered to:

- i. An internally managed, security patch and vulnerability Alert/ticket notification (like SDM) must be established within Ncell.
- ii. All vulnerabilities identified from scanning activities shall be reported to the application & asset owner:
 - a. Raise tickets for external critical & high-risk vulnerabilities to concerned stakeholders within 48 hours of identification.
 - b. Raise tickets for external medium or low risk vulnerabilities to concerned stakeholders within 7 days of identification.
 - c. Send email for internal vulnerabilities (all severity), to concerned stakeholders within 48 hours of identification.
- iii. Asset Custodians must subscribe and respond to internally managed security patch and vulnerability ticket.
- iv. Application & asset owners shall be provided access to vulnerability scanning reports for systems under their responsibility.
- v. Reports will be provided to Ncell executives to describe the overall risk in the environment. Reports shall include high level information including number of vulnerabilities identified in the environment,

Ncell	Ncell	Classification: Internal
	Vulnerability and Patch Management Procedure	Owner: CIO/Head of IT
		Effective Date: 15 th August, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

historical trending of vulnerability numbers, categories or types of vulnerabilities, and historical remediation response time frames.

5.4 Vulnerability Remediation

The following controls should be adhered to:

- i. Vulnerability remediation shall be completed in accordance with below mentioned timelines for external vulnerabilities.
 - a. Critical risk vulnerabilities - 48 hours
 - b. High risk vulnerabilities – 120 hours
 - c. Medium risk vulnerabilities – 720 hours
 - d. Low risk vulnerabilities – To be fixed by next scanning (Quarterly) cycle
 - e. Vulnerabilities related to kernel – to be closed maximum two times in a year.
- ii. Vulnerability remediation shall be completed in accordance with below mentioned timelines for internal vulnerabilities for Minimum Crown Jewels, Crown Jewels.
 - a. Critical risk vulnerabilities – 14 days
 - b. High risk vulnerabilities – 30 days
 - c. Medium risk vulnerabilities – 90 days
 - d. Low risk vulnerabilities – 180 days.
 - e. Vulnerabilities related to kernel - to be closed maximum two times in a year.
- iii. Vulnerability remediation should be performed in accordance with Ncell's change management procedure.
- iv. Remediation may take the form of patching, configuration update, and/or removal of the technology resource (disabling functions or removing computing systems/devices from Ncell's network).
- v. When remediation cannot be accomplished using patching, configuration update, or removal of the technology resource, an alternative mitigation strategy should be developed by the resource owner and approved by Head of IT. Alternative strategies may take the form of network access restrictions, real-time asset monitoring, or other appropriate strategy.
- vi. An audit log should be kept for all actions performed towards vulnerability remediation.
- vii. On successful patching of identified vulnerabilities, confirmation should be given by the application/asset owner to the security team and the corresponding ticket should be closed.
- viii. Functional teams should perform re-scans/clean scans to ensure successful closure of vulnerabilities patched by the functional teams and report the same to the concerned stakeholders.

5.5 Patch Management Cycle

- i. Monthly Security patches shall be applied, where applicable, on all systems OS by respective teams with the authorization of system / service owners and shall be scanned regularly for vulnerability management by security team.
- ii. It shall be ensured that the following patch levels are maintained for all systems:
 - a. Support structure for IT Assets: Minimum of *N-2 Major release supportability.
 - b. Support structure for Telco Assets: Minimum of *N-4 Major release supportability.

*N being the latest Major Release supported by the vendor.

5.6 Independent Reviews

The following controls should be adhered to:

- i. Periodic technical vulnerability reviews by an independent supplier shall be conducted for Ncell's applications and infrastructure components, identified based on risks associated with them.
- ii. An independent penetration agent or penetration team shall:
 - a. Conduct a vulnerability analysis on Ncell systems.
 - b. Perform internal/external penetration testing for crown jewels at least annually based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.

Ncell	Ncell	Classification: Internal
	Vulnerability and Patch Management Procedure	Owner: CIO/Head of IT
		Effective Date: 15 th August, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

5.7 Deployment of New Systems

The following controls should be adhered to:

- Any newly built IT Asset should be hardened as per Ncell's Minimum Baseline Security Standards (MBSS) before being deployed into the production environment.
- All newly built systems must be patched prior to being issued to an end-user.
- Any newly built IT Assets must be fully patched as part of the asset build process and not placed on a production network until fully patched.
- Vulnerability scanning of newly built IT Assets should be performed in advance of placing the IT Asset into a production hosting facility.

6. Management Reporting

The following KPIs should be calculated and reported during the management reporting process:

S.No.	Ownership	KPI	Calculation
1	Information Security Team	Number of VA scans performed.	Number of scans performed / Number of scans planned
2	Information Security Team	Frequency of penetration tests conducted.	Number of Penetration tests performed / Number of Penetrations Tests planned
3	System Owners	Number of vulnerabilities patched within defined SLAs.	Number of vulnerabilities remediated within SLA / Number of vulnerabilities identified

7. Governance and Compliance

- Exception management process shall be followed to raise the exception for this procedure.
- Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.
- Vulnerability and patch management reports and records shall be maintained and protected from unauthorized accesses.

8. Associated Documents

- Information Security Policy
- Change Management Procedure
- Incident Management Procedure