NWC OT Cybersecurity Patch Management Procedure

Document Number:	A01001045-PRO-PAM
Issue Date:	August 16, 2021
Revision Number:	01
Issued For:	Approval

Revision Details

Name	Title/Dept.	Signature	Date
Prepared by:			
Sidrat Mehreen	Senior OT cybersecurity Analyst		August 10, 2021
Reviewed by:			
Sameen Ullah Khan	OT Cybersecurity Lead		August 12, 2021
Approved by:			
Farhan Rasheed	Operations Manager		August 14, 2021

Issued by:			
Syed Ali Raza	Planning Engineer		August 16, 2021

History Page

Issue No.	Issue Date	Prepared By (Name)	Reviewed By (Name)	Owned By (Name)	Endorsed By (Name)	Approved By (Name)
00	July 15, 2021	Sidrat Mehreen	Sameen Ullah Khan			Farhan Rasheed Khan
Change Description						
Change Description						
Change Description						

Reference Documents

Document Number	Document Title
ECC-1:2018	National Cybersecurity Authority Essential Cybersecurity Controls (NCA ECC)

Document Roles and Responsibilities

	Prepare/ Update/ Amend	Review	Approve	Publish
Owner	YES	YES		
Cybersecurity Steering Committee		YES		YES
Corporate Strategy & Performance Management VP			YES	

Table of Contents

Glossary

Word or Phrase	Explanation
Asset	General support system, major applications, resources, high impact program, physical plant, or a logically related group of systems
Asset Register	Location, condition, owner, status, procurement dates, depreciation or values of the assets
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.
Backup	Copying data to protect against loss of Integrity or Availability of the original.
BU	Business Unit- Represents a specific line to the business and is a part of firm's value chain of activities including operations, accounting, HR, marketing and sales.
Central Patch Management system	A database where all asset owners will update and maintain current level of patching. It will also check compliance status when it comes to patching.
Change Request Form	The change request form is the primary tool used for requesting, approving, and documenting changes to the project and is an important piece of the change management process (here referring to change management procedure)
Compliance	Ensuring that a Standard or set of Guidelines is followed. A means of conforming to a rule, such as a specification, policy, standard or law.

Word or Phrase	Explanation
firmware	Tangible computing device providing low level of controls, held in non-volatile memory devices such as ROM, EPROM, Flash memory
Integrity	The property of safeguarding the accuracy and completeness of assets.
Panorama	centralized management system that provides global visibility and control over multiple Palo Alto Networks next generation firewalls
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Test Environment	A controlled Environment used to test Configuration Items, Software Builds, OT/IT Services, Processes, etc.
WSUS	Windows Server Update Services

1. Introduction

This document provides the procedure necessary to maintain the availability and integrity of OT systems and data by applying the latest operating system and application security updates/patches in a timely manner, and to establish a baseline methodology and time frame for patching and confirming patch-management compliance.

This procedure is applicable to all NWC OT infrastructure.

2. Roles and Responsibilities

Roles	Responsibilities
OT Asset Owner	OT Asset Owner shall have the responsibility of: • Determining current version of patches • Determining latest version available from vendors • Initiation of patching
SCADA O&M Team	SCADA O&M Team shall have the following responsibilities, not limited to: • Provide list of vendor approved windows updates as published by vendor • Provide Timing at which the patching is to be done manually • provide grouping of SCADA systems based on Asset location, Operating System & Installed Softwares for deployment approval • All updates to be deployed using Change Management Process • Update central patch management system
OT Admin	OT Admin shall have the following responsibilities: • Approval of patch deployment of Windows OS for each group based on validated patches from SCADA O&M Team • Execute the required Actions for patch management as received against Change Request Form in WSUS

Roles	Responsibilities
	• Push updates from WSUS server to SCADA servers and workstations • Update central patch management system
Smart Operations Team	Smart Operations Team shall be responsible for: • Initiate change request for firmware upgrade for Level 0-1 devices • Perform Backup if scheduled or manual backup has not been performed • Upgrade firmware of Level 0-1 devices • Update central patch management system
Infrastructure Team	Infrastructure Team shall: • Perform Backup if scheduled or manual backup has not been performed • Install latest patches on Physcial and virtual servers • Update central patch management system
BU Network Team	BU Network Team shall be responsible for: • Initiate change request for patching/updating network devices • Perform Backup if scheduled or manual backup has not been performed • Upgrade firmware of network devices • Update central patch management system
IT Helpdesk	• Perform Backup if scheduled or manual backup has not been performed • Install/implement patches for Workstations and standalone machines • Update central patch management system

3. Patch Management Procedure

Guidance Notes:

1: All patch management procedures shall follow change management process.

2: Updates/patches must be done after approval of change request.

3: updates and patching must be done after establishing backup and recovery mechanism.

4: Record of all updates shall be maintained in central patch management system.

5: All patching/updates must be done as per OEM and vendor recommendations.

6: All patching/updates must be scheduled to reduce operational impact.

7: All the updates/patches installed are logged and updated manually in Central Patch Management System whether successful or not.

3.1 Workstations

1. SCADA O&M will update central patch management system with applicable vendor approved patches and updates.
2. SCADA O&M team will initiate change request for deployment and installations of the applicable vendor approved patches/updates.
3. IT Helpdesk will create backup and recovery mechanisms.
4. OT Admin will push applicable vendor approved Windows patches to OT workstations using WSUS.
5. IT Helpdesk install/implement patches for Workstations.
6. IT Helpdesk shall restore OT workstations to its original state in case of major failures by any restoration mechanism adopted in step 3.
7. IT Helpdesk shall update central patch management system with current status of patching activity.

3.2 Servers

1. Infrastructure Team initiates the request for approval of patches/updates on OT servers after receiving the list of vendor approved patches/updates from SCADA O&M team.
2. Infrastructure Team will create backup and recovery mechanisms.
3. OT Admin will push applicable vendor approved Windows patches to Servers using WSUS.
4. Infrastructure Team will Install latest patches on Physcial and virtual servers.

5. Infrastructure Team shall restore OT workstations to its original state in case of major failures by any restoration mechanism adopted in step 3.
6. Infrastructure Team shall update central patch management system with current status of patching activity.

3.3 Network Hardware/Devices (Routers, Switches, etc.)

1. Network Team initiates the request for approval of firmwares on network devices
2. Network Team will create backup and recovery mechanisms. Network Team must take backups.
3. Network Team will upgrade firmware of network devices.
4. Network Team shall restore OT workstations to its original state in case of major failures by any restoration mechanism adopted in step 3.
5. Network Team shall update central patch management system with current status of patching activity.

3.4 Level 0-1 Device Firmware Updates

1. Smart Operations will create backup and recovery mechanisms.
2. Smart Operations will Upgrade firmware of Level 0-1 device.
3. Smart Operations shall restore OT workstations to its original state in case of major failures by any restoration mechanism adopted in step 3.
4. Smart Operations shall update central patch management system with current status of patching activity.

3.5 Standalone Systems

1. Standalone systems in OT environment will be segregated upon the type, as follows:
    a. Laptops/ workstations
    b. Network devices
    c. Level 0-1 devices
    d. Servers
2. A list of vendor approved windows update as published by the vendor will be obtained from SCADA O&M team.
3. OT Admin will be responsible for pushing the patches/updates using approved medium.
4. IT helpdesk will take backups and install the updates/patches on the assets.
5. The Respective OT Asset Owners are given as:
    a. If windows machine (Workstations) SCADA O & M team will initiate request for updates/patches.

b. If servers, Infrastructure team
c. If Network devices, Network team
d. If Level 0-1 devices, Smart Operations team

6. In case of any failure during patching process, backup and recovery is implemented, already documented, and communicated to OT Asset Owners.

3.6 Process

Activity		Procedure
1.1	Current and latest update/patch/firmware version determination	OT Asset Owner will determine the current version on the systems and also the latest updates/patches/firmware for vendors.
1.2	Vendor approved updates/patches/firmware	A list of vendor approved updates/patches/firmware as published by the vendor.
1.3	Initiate updates/patches/firmware process	OT Asset Owner initiates the process for updates/patches/firmware by submitting a change request form.
1.4	Change Management Approval	Change Manager will approve the change request form upon receiving the form and evaluates updates/patches/firmware with compliance to Change Management Procedure.
1.5	Backup and Recovery process	Respective team will create backup and recovery mechanisms.
1.6	Pushing patches/Updates from Vendor	OT Admin will push applicable vendor approved Windows patches/updates to Servers using WSUS.
1.7	Implement the updates/patches/firmware	Respective team will implement updates/patches/firmware

1.8	Backup and Recovery process (In case of failure)	If updates/patches/firmware are unsuccessful due to any reason, backup and recovery of the system will be performed with informing respective Team.
1.9	Close the process	The process will be closed by updating the Central Patch Management System.

3.7 Patches Updates Frequency

These durations are typical and Stakeholders shall determine frequency of update/patching based on criticality, vulnerabilities, location, and other aspects for every asset in OT Asset Inventory.

Types of patches	Time Period
Workstations and Servers	Vendor Recommended or 3 months release unless critical update required
Network Devices	Vendor Recommended or 1 year release unless critical update required
Level 0-1 Devices	Vendor Recommended or 2-3 years release unless critical update required

4. Exception Handling

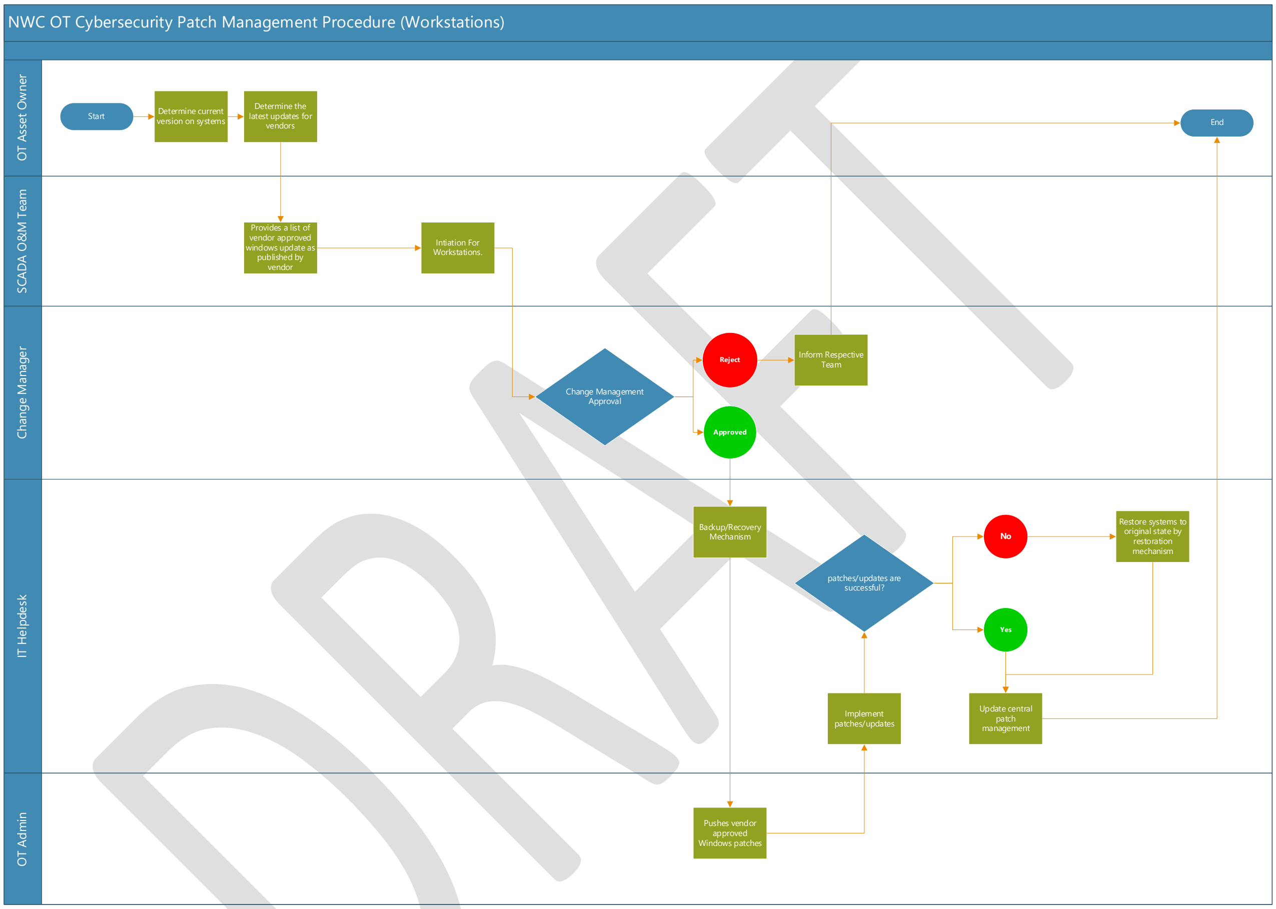
1. Exceptions must be approved during the change management process.
2. Risk assessment/Vulnerability will be a part of the change management but subject to approval from CAB.

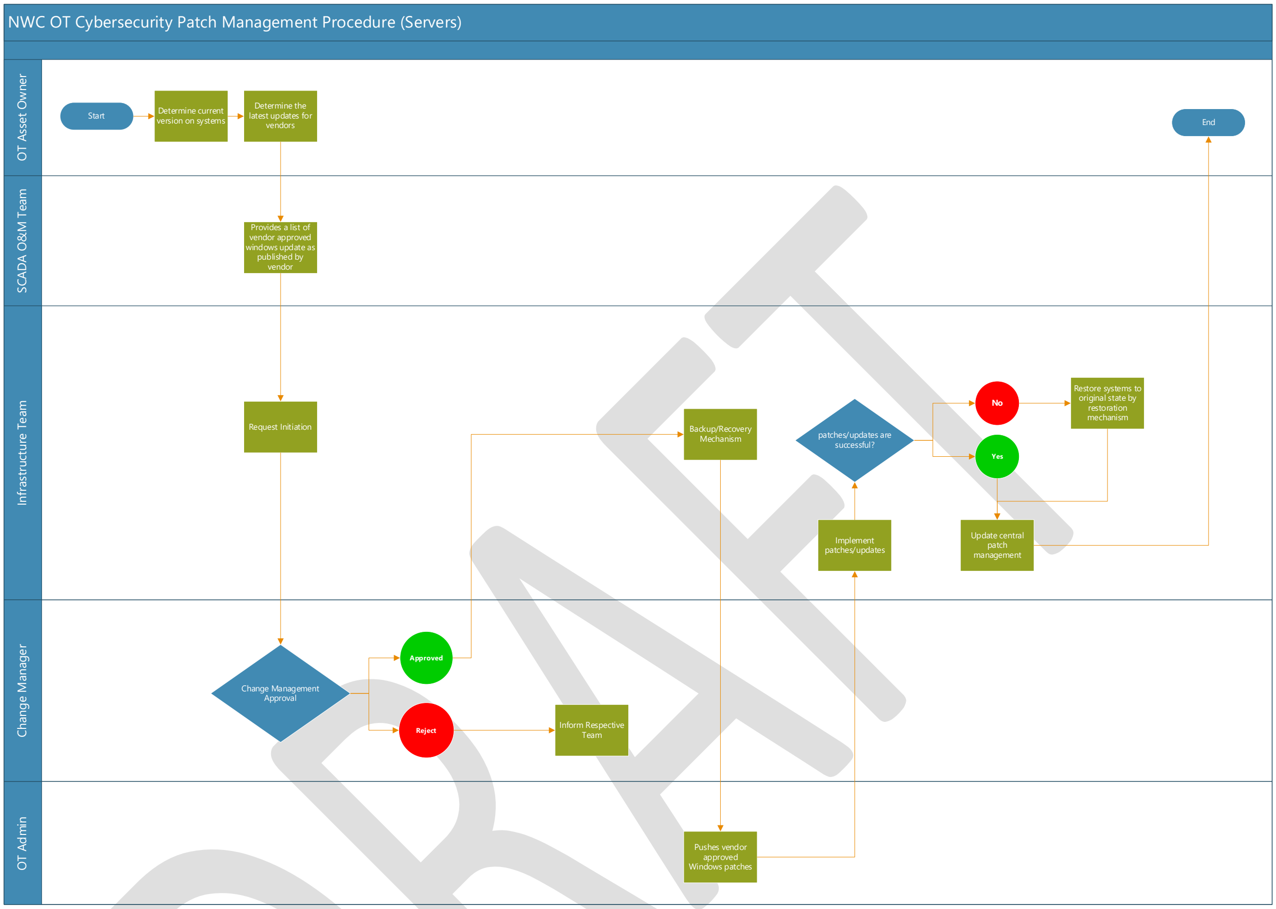
5. Patch-Compliance Review

1. Patch Management Compliance tracking shall be done using Central Patch Management System.
2. OT Admin shall generate and review patch management/compliance reports at least monthly from the central patch management servers for windows.
3. A central patch management system shall be maintained manually for Level 0-1 and Standalone Devices updates.

4. In reviewing the patch reports, respective Stakeholders will identify un-patched machines that connect to the OT network and either patch or define an exception.
5. The compliance of the patch management systems shall be done annually.

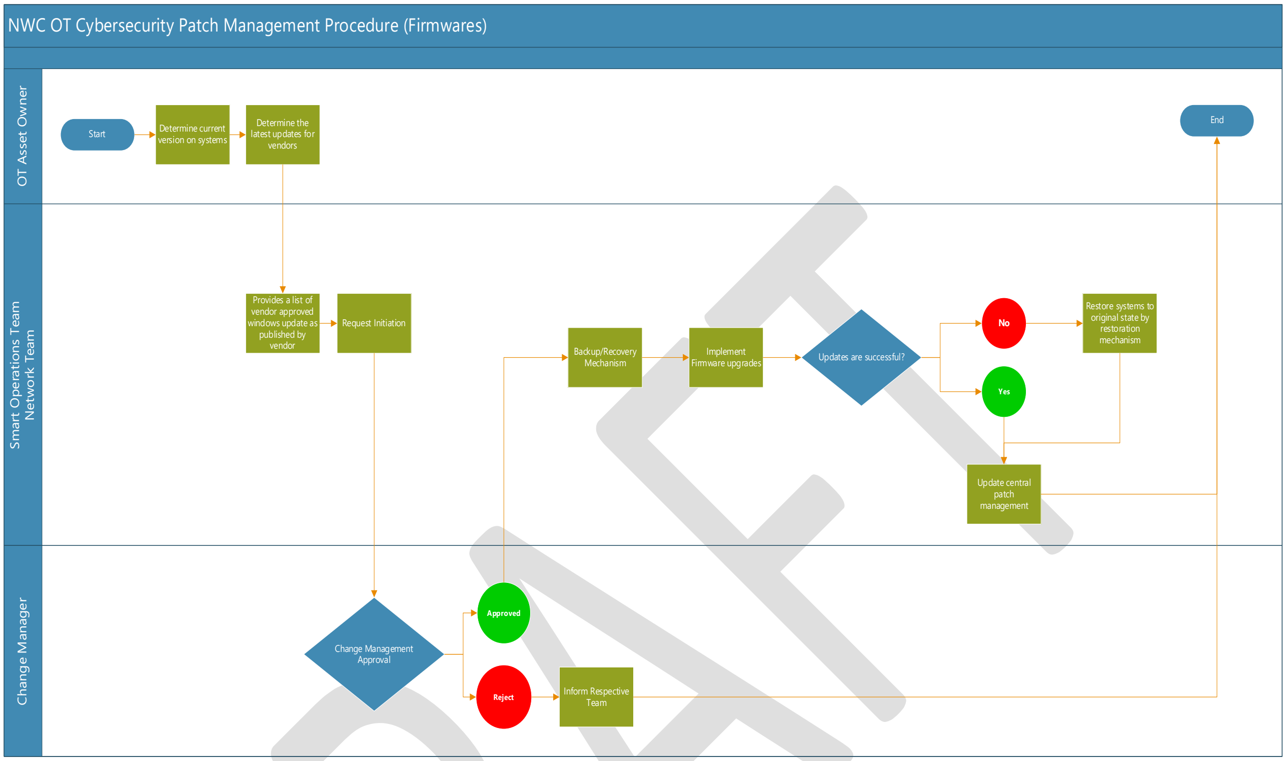
6. Process Flow Chart


NWC OT Cybersecurity Patch Management Procedure (Workstations)
OT Asset Owner
SCADA O&M Team
Change Manager
IT Helpdesk
OT Admin
Start
Determine current version on systems
Determine the latest updates for vendors
End
Provides a list of vendor approved windows update as published by vendor
Intiation For Workstations.
Change Management Approval
Reject
Inform Respective Team
Approved
Backup/Recovery Mechanism
patches/updates are successful?
No
Restore systems to original state by restoration mechanism
Yes
Implement patches/updates
Update central patch management
Pushes vendor approved Windows patches


NWC OT Cybersecurity Patch Management Procedure (Servers)
OT Asset Owner
SCADA O&M Team
Infrastructure Team
Change Manager
OT Admin
Start
Determine current version on systems
Determine the latest updates for vendors
Provides a list of vendor approved windows update as published by vendor
Request Initiation
Change Management Approval
Approved
Reject
Inform Respective Team
Backup/Recovery Mechanism
Pushes vendor approved Windows patches
Implement patches/updates
patches/updates are successful?
No
Yes
Restore systems to original state by restoration mechanism
Update central patch management
End

PROPRIETARY NOTICE

THIS DOCUMENT CONTAINS INFORMATION PROPRIETARY TO NWC. ANY DISCLOSURE OR USE THEREOF IS EXPRESSLY PROHIBITED EXCEPT UPON THE WRITTEN PERMISSION OF NWC.


NWC OT Cybersecurity Patch Management Procedure (Firmwares)
OT Asset Owner
Smart Operations Team
Network Team
Change Manager
Start
Determine current version on systems
Determine the latest updates for vendors
End
Provides a list of vendor approved windows update as published by vendor
Request Initiation
Backup/Recovery Mechanism
Implement Firmware upgrades
Updates are successful?
No
Yes
Restore systems to original state by restoration mechanism
Update central patch management
Change Management Approval
Approved
Reject
Inform Respective Team