




## Procedure for Network Patch Management

TIM-PR024, Ver 1.2

DocuSigned by:  
  
9BB6619E2FFC443...

---

## Table of Contents

1.	OVERVIEW.....	3
2.	SCOPE.....	3
3.	APPROCH & CONSIDERATION.....	3
4.	ACRONYMS AND DEFINITIONS.....	4
5.	REGULAR PATCH MANAGEMENT PROCEDURE .....	4
6.	PATCH DEPLOYMENT TIMELINES (BUSINESS-AS-USUAL SCENARIO) .....	4
7.	PATCH MANAGEMENT TIMELINES FOR CRITICAL/EMERGENCY SCENARIO .....	5
8.	ROLES AND RESPONSIBILITIES .....	5
9.	PATCH TESTING .....	5
10.	PATCH CATEGORY DEFINITION AND TIMELINES .....	6
11.	PATCH MANAGEMENT ADMIN REVIEW .....	6
12.	DOCUMENT HISTORY .....	7
13.	APPENDIX.....	7
14.	ANNUAL REVIEW HISTORY .....	7

## **1. OVERVIEW**

TIM needs to evaluate Network devices IOS running in the network on regular basis and mitigate the risks identified as part of review by upgrading/downgrading Network devices IOS which are in scope.

## **2. SCOPE**

Critical devices as following which hold critical configuration details like routing information, quality of service details, access control list, VLAN information:

- Core Routers
- Core Switches
- Distribution Switches
- Wireless LAN Controllers

### **Out-of-Scope:**

- Non critical devices like layer-2 access switches which do not hold any intelligent controls like routing, Quality of Service, Access-control, VLAN details list etc.
- Customer owned or managed network devices
- *Out of scope Caveat:* If OEM declares there is a security bug in L2 Switch IOS with high impact and there is no alternate/workarounds, IOS/OS can be upgraded post discussion/review with Change Advisory Board (CAB).

## **3. APPROCH & CONSIDERATION**

While considering defined SCOPE and Dependencies, we will be following well-known industry standard best practice approach of Evaluate, Test, Approval, Deploy and Verify while applying our agreed baseline of (N-2). Baselines should be decided based on factors like MAJOR RELEASE and N-2, looking at CIS benchmarks as well as current stability on IOS / Patches (Wherever applicable) along with domain leads approval.

- **Evaluate**
  - Critical Inventory of the assets.
  - Monitoring for MAJOR patches and vulnerabilities, remediation and Threats.
  - Prioritizing MAJOR Release patches / IOS / Vulnerability Remediation's.
- **Approval, Test & Deploy**
  - Get theses patches approved from OEM, Domain Head and as per criticalities and internal Change management process.
  - As mentioned in Patch testing section 9, patch should be tested as per feasibility of the test environment, which is subject to Hardware availability. If the hardware is not available Security team will use information provided by OEM/Partner/Technical assistance center (TAC) and upgrade the OS IOS accordingly
  - In most of the cases as there are limitation of test environment, so patches should be first deployed on secondary appliances (Passive Device) to observe any functional abnormality before deploying on primary appliances.
  - Implement respective IOS / patches as part of change implementation plan.
- **Verify**

## PROCEDURE FOR NETWORK PATCH MANAGEMENT

- Verify respective IOS / patches functional impact as part of post implementation plan for change management process.

Patches needs to be installed on critical services have MAJOR dependencies and subjected to approval and **DOWNTIME** from location **OICs** and **projects** for Implementing and testing. This one of the most important criteria for major IOS / Patch / Firmware deployment.

As this will be continuous task and a part of continuous improvement all the devices below baseline or benchmark should be updated in tracker with status of successful / failure of the patches along with Dependency, Plan of Action, Target Date, and Current Status along with approvals from Domain Lead. This free format report is stored in Central Repository for Security Team. Sample format of few fields are shown in Section 11.

**Note:** Baseline approach is used as indicative with intention of making sure that all the critical devices are not on old and absolute IOS / Patches, implementing all the appliances on baseline will not be mandatory if existing IOS / Patches did not have any vulnerabilities and already validated in internal Vulnerability scanning conducted via. ISG.

#### 4. ACRONYMS AND DEFINITIONS

Term/ acronym	Explanation
TIM	Technical Infrastructure Management
SLA	Service Level Agreement
CAB	Change Advisory Board
KDB	Knowledge Database
SPOC	Single Point of Contact

#### 5. REGULAR PATCH MANAGEMENT PROCEDURE

- Business as usual scenario IOS/OS management for in-scope network devices will be reviewed once in six months
- Review results will be shared with TIM Network head for approval on implementation plan to mitigate risks reported
- OEM Partner will be consulted and requested to provide recommendations on the IOS/OS report applicability and IOS/OS recommendations
- OEM Partner will communicate to TechM with their recommendations and seek sign off with Network Leads.
- TIM will implement recommendations in a phased manner with Change management procedure being followed based on severity and urgency
- TIM will close the IOS/OS review report with comments and action plan if any for initial 6 months.
- TIM will save the detail in free format report stored in Central Repository. Sample format of few fields are shown in Section 11.

#### 6. PATCH DEPLOYMENT TIMELINES (BUSINESS-AS-USUAL SCENARIO)

- IOS/OS will be implemented post CAB approvals in standard timelines above.
- Standard IOS upgrade requirements will be mitigated across organization in 8 to 12 weeks post IOS report is published with in TIM and TIM Network head approvals.

## PROCEDURE FOR NETWORK PATCH MANAGEMENT

### 7. PATCH MANAGEMENT TIMELINES FOR CRITICAL/EMERGENCY SCENARIO

- Emergency requirements that have security risks and which demand patch deployment functionally to work will be deployed in Two weeks post CAB approvals.
- In rare cases if equipment IOS cannot be upgraded during emergency, network team will inform the change advisory board and work with other departments to apply work-around solutions to protect the TechM network.

Note: Refer Section Nine for detailed patch category definition and timelines.

### 8. ROLES AND RESPONSIBILITIES

- L1 Network Engineers, as per IOS audit checklist will review the network once in 6 months as per calendar schedule
- L2 Network Engineer will review the IOS audit report and discuss with Network managers for patch deployment
- L3 Network Engineer will validate the report with OEM partner for IOS applicability and feasibility.
- TIM will obtain CAB approvals based on applicability and importance.
- TIM will deploy the suggested patches as per schedule

Task / Activity	ISG	Security TIM	CAB	Process TIM	OIC	Business Owner	Vendor / OEM
Procedure ownership, development & maintenance	C	R, A	-	C	I	I	-
Define time line metrics.	R	C, A	-	C	-	C	-
Periodic reviews of patches	I	R, A	C, I	I	I	-	C
Feasibility / Applicability checking.	-	R, A	-	-	-	-	C, R
Evaluation, testing for applicable patches	-	R, A	I	I	-	-	C
Inform ISG about pre and post patch implementation for VA Scans and reports.	I	R, A	C, I	-	I	-	C
Approvals for applicable patches.	C	R, I	R, A, I	I	I	I	-
Vulnerability scanning, analysis, assessment, reporting pre and post patch implementation.	R, A	C, I	I	I	I	-	-
Patch Deploy / implementation and closure.	I	R, A	C	I	I	I	-

### 9. PATCH TESTING

- Network team wherever feasible will test IOS prior to deployment subject to test hardware availability
- If the hardware is not available, network team will use information provided by OEM/Partner/Technical assistance center (TAC) and upgrade the IOS accordingly
- Post upgrade service will be monitored for 24~48 hours for any abnormal behavior and further action would be taken accordingly.

## PROCEDURE FOR NETWORK PATCH MANAGEMENT

### 10. PATCH CATEGORY DEFINITION AND TIMELINES

Patch Categories	Patch Category Description	Examples	Recommended Time Frame
High P1	Vulnerability that impacts critical business processes and having security risks. It cannot be avoided or it is significant, all necessary systems must be patched. The vulnerability is categorized high if no workaround is available or rated by product owner/ security advisories.	Business critical devices - Internet facing, Routers, Core Switches etc.	Two Weeks post E-CAB approval.
Medium P2	Vulnerability that will have moderate impact to business or recommendation to patch by OEM or security advisories.		4 to 5 Week post analysis done on recommendation
Low P3	Not an imminent vulnerability or it is one that will have minimal impact to non-critical systems. Standard IOS upgrade requirements will be mitigated across organization.		8 to 12 week post IOS/OS analysis done

### 11. PATCH MANAGEMENT ADMIN REVIEW

Sr.No.	Device Details	Device Roll	Location	Hotfix/Firmware Version		Reviewed/Approved Date	Reason for Upgrade	Remarks
				Present	Proposed			

\*As mentioned in Section 4 this is the free format report which is being maintained by team and stored in centralize repository. The data which is being maintained is not limited to the format shown above.

## PROCEDURE FOR NETWORK PATCH MANAGEMENT

### 12. DOCUMENT HISTORY

Version	Date	Author (function)	Reviewed by	Approved by	Nature of changes
Issue 1.0	20/05/2015	Dayanand Kudari/Narender Ganji	ISG/Dhananjay S./Neeraj P	Sharad Shanbhag	First Integrated Issue
1.1	07/08/2015	Dayanand Kudari	Neeraj Pathak	Sharad Shanbhag	Bi-annual review. No changes.
1.2	22/09/2017	Yogesh Gavane	Abhimanyu Sethi, ISG, Viteswar Tyagi	Prasanna Aklkar	Reviewed and changes done to make it vendor generic document and some other changes.

### 13. APPENDIX

NA

### 14. ANNUAL REVIEW HISTORY

Annual Review Conducted On	Version Reviewed	Is Change Required (Y/N)	Document Uploaded in BMS (Date)	Remarks
6/03/2017	1.1	N	13/3/2017	Annual Review
10/05/2018	1.2	N	11/05/2018	Annual Review
5/08/2019	1.2	N	06/08/2019	Annual Review