Ministry of Communications & Information Technology

Patch and Vulnerability Management Standard

Table of Contents

1 Introduction

1.1 Purpose

Patching systems, applications and devices promptly is an essential part of an effective approach to cyber security. It ensures that known problems and vulnerabilities that could be exploited by cyber attackers and which may impact the availability, integrity, and confidentiality of our information assets are remediated promptly.

This standard details the requirements for patch and vulnerability management throughout the Government of Samoa (GoS). It aims to establish a unified patching process across all identified applications and system software in GoS.

1.2 Scope

The requirements in this standard apply to all application software used by end users, as well as software that resides on GoS hardware (servers, desktops, laptops, switches, routers, storage devices, etc.) maintained by the GoS. It also applies to patching of systems where these are being managed by a third party, such as a cloud service provider.

This Standard must take into account the upgrading of core security infrastructure components such as the SIEM and its interrelated components due to the following:

- Security infrastructure downtime
- Large configuration changes between versions
- Reconfiguration of component interconnectivity

The hardware and software excluded from this standard are:

- Internally produced custom code and software that has been approved by the Ministry of Communication, Information and Technology (MCIT))for use, and has provided along with it a maintenance procedure to reduce vulnerabilities); and
- Vendor product upgrades, (e.g. upgrading to newer windows, which will follow a separate upgrade program)

No other GoS systems are considered to fall outside the scope of this standard unless an exemption has been sought and approved by the MCIT.

A justification must be provided to the MCIT for a risk-based assessment, and subsequently approved by the CEO. It must then be recorded in the Government risk register.

2 Principles

2.1 Principles guiding our Patch & Vulnerability Management

The following table outlines the overarching principles that govern the approach to patching at the GoS.

Patching of the network components must follow this Standard

- All components of the network should be adhering to the patching and vulnerability management procedures that are deemed relevant. Understandably, our environment is diverse, and there may be slight variations in network components, but all should have follow this Standard to ensure consistency and a common understanding;
- In addition, the SIEM and supporting network components should follow the patching process for these systems and their updates (minor point releases) and upgrades (major point releases); and
- Upgrades are not recommended as the configuration differences between different versions of security infrastructure components vary drastically. This process should follow a system change management plan to mitigate associated risks before implementation.

Patching across the entire IT environment

- Neglecting to patch even one system can leave the whole environment vulnerable. We are focussed on knowing and tracking all systems within our IT environment, and including them all in our patch management program.

Adopt a risk-based approach to patching

- We employ a risk based approach to patching systems. There is a trade-off between being vulnerable to malicious software and the effort and potential disruption to business operations required to perform patching – particularly for less critical patches.

Wherever possible, automate patching

- Automated tools used for patching must be suitable to the size and complexity of the GoS IT environment.

Patching approaches require minimal end-users involvement or disruption to business operations

- Patching must, wherever possible, be applied without requiring end-user intervention, or disruption to business processes. Communications and planning will be conducted to ensure this is done as best as possible.

3 Patch Management Roles & Responsibilities

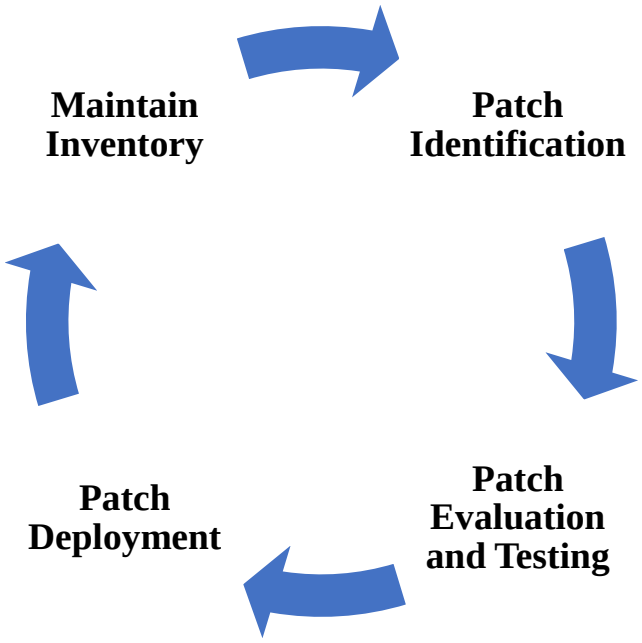
It is important that responsibilities for various aspects of patch management within the GoS are assigned to appropriate personnel, and their responsibilities understood and they are appropriately tasked (skilled and authorised) to carry out the identified responsibilities.

Role	Responsibility
ACEO / Principal / Manager of ICT	• Assessment of risks associated with the application (or non-application) of patches, and escalation of risks for review in accordance with GoS's risk management acceptance criteria.
ICT Team with advice from MCIT (ICT & SamCERT)	• Review and assess vendor-released patches and their suitability for potential deployment within the GoS IT environment; • Identifying pilot group(s) within GoS for the testing of patches, if required; • Deploying patches to the pilot group for functionality testing; • On successful completion of the pilot group testing, deploying patches to the rest of the organisation, (if deemed appropriate); • Responding to all identified issues once patches have been deployed and (having a roll back procedure ready); • Conducting update testing on an isolated network replica for security infrastructure components (e.g. SIEM connected applications); and • Ensure auto-update features are applied, authorised for use and enabled on all software applications.
SamCERT	• Advise on patch criticality and the importance of patch deployment.
User	• Complying with all patch requirements of the GoS and contained within this Standard.
Procurement Officer (with guidance from the MCIT ICT & SamCERT)	• Ensure that the requirements of this Patch Management Standard are also enforced against third third party suppliers (e.g. cloud service providers).
The MCIT and CEO	• Provide the approval of exemptions request, (in conjunction with business owners), for the non-application of patches forto specific sysystems/applications that cannot be patched due to specific business reasons. Justification must be provided to the MCIT for a risk-based assessment, and subsequently approved by the CEO.
Corporate services	• Populate the asset register with information on the newly deployed system and software.

4 Requirements for Patch Management

The Patch Management Lifecycle outlined in the illustration below describes the key phases involved in the effective application of patches in a timely fashion within the GoS.

The remaining sections of this Standard broadly outline the requirements that apply for each of the four (4) stages of the Lifecycle.



4.1 Maintaining the Inventory

Appropriate IT Asset Management through the maintenance of an asset inventory provides helpful insight into the level of exposure GoS has as a result of a particular hardware or software vulnerability, and the potential impact if that hardware or software is not patched.

The use of an inventory is an important pre-requisite to the remaining steps of the Patch Management Lifecycle because its existence enables GoS to assess what patches are relevant to its IT environment based on current systems and software in use.

As such, some requirements have been put forward to ensure that inventory maintenance is sufficient.

1. **An asset inventory must be maintained**

An inventory of all system and software types must be recorded and maintained by each GoS Ministry. This inventory will be populated by each Ministry by scanning the network to identify all systems for inclusion.This ensures the scope for patching is understood and technical vulnerabilities are managed effectively.

2. **System details must be recorded in an asset register**

The following details about each system must be recorded in each Ministries asset register:

- Computer name, asset tag, criticality and location;
- IP address / DNS Name;
- Software installed along with its version;
- End of Life (if applicable);
- Support details; and
- System owner.

3. **Asset inventory management practices and tools must be applied (where appropriate)**

Asset management and inventory tools must be used to help with the collection of hardware properties (CPU, BIOS, disks, networking devices, etc.), software installed and warranty information.

4. **Regular scanning of the IT environment must be undertaken to ensure inventory is complete**

To ensure completeness and accuracy of the inventory, each Ministry's ICT division must scan their IT environment on a quarterly basis, at a minimum, to identify all systems fo inclusion in the patch management process.

Documentation and reports of these scans taken place should be maintained and recorded. In the event they are requested, they can be used as evidence demonstrating diligence with the Patch & Vulnerability Management requirements.

4.2 Patch Identification

The purpose of the Patch Identification phase of the lifecycleis to ensure that a coordinated process is in place to facilitate the prompt identification of available patches. This is a critical step towards ensuring the patchesare evaluated and, where appropriate, deployed within the GoS IT environment.

As such, the following requirements are to be in place:

1. **Methods for receiving vendor notifications must be established**

A method for receiving vendor notifications regarding newly available patches must be established for all IT systems and hardware. This is generally achieved by monitoring and subscribing to the advisories released by the vendor.

2. **Vendor patch bulletins must be reviewed prior to patch deployment**

Prior to deployment, vulnerability and patch related information published by the vendor must be reviewed before deploying patches within the IT environment.

This will be done by the ICT teams of each Ministry, unless deemed a 'critical security patch', in which case this will be reviewed by the SamCERT.

Vulnerability and patch related information that must be reviewed includes:

- A list of products and versions affected;
- Technical details of the vulnerability including an overview of how exploitation occurs;
- Typical consequences of exploitation: code execution, information disclosure, denial of service etc.
- Current exploitation status: whether the vulnerability is being exploited;
- The existence and details of any temporary workarounds; and
- An overall measure of severity based on the above factors (e.g. based on risk appetite and known severity scales).

In addition to individual vulnerability/patch details, some vendors publish a consolidated bulletin which also includes the vendor's recommended patch deployment order. If available, this information should also be reviewed.

3. Regular internal vulnerability scanning must be completed

Within the internal GoS IT environment, internal scans must be completed quarterly to ensure that systems meet the required patching baselines, and to assist in the identification of security patches that should be in place but are missing.

Where internal vulnerability scans identify missing patches these must be actioned as a matter of priority.

The following guidelines below are best practice timeframes for conducting vulnerability scans for missing application patches[1]:

Threat Type	Timeframe
Basic	**Internet-facing services:** daily **Commonly-targeted applications:** fortnightly **Other applications:** as required
Moderate	**Internet-facing services:** daily **Commonly-targeted applications:** weekly **Other applications:** fortnightly
Advanced	**Internet-facing services:** daily **Commonly-targeted applications:** weekly **Other applications:** fortnightly

The following guidelines below are best practice timeframes for conducting vulnerability scans for missing operating system patches[2]:

[1] Australian Cyber Security Centre, *Assessing Security Vulnerabilities and Applying Patches* (2021)
[2] Ibid.

Threat Type	Timeframe
Basic	**Internet-facing services**: daily **Workstations, servers, network devices & other network-connected devices**: fortnightly
Moderate	**Internet-facing services**: daily **Workstations, servers, network devices & other network-connected devices:** weekly
Advanced	**Internet-facing services**: daily **Workstations, servers, network devices & other network-connected devices**: weekly.

4. **Auto-update features on applications authorized for use within the GoS must be enabled**

To facilitate the prompt identification of patches that are appropriate for deployment, the auto-update feature for all software applications authorized for use within GoS must be enabled.

4.3 Patch Evaluation and Testing

It is important the patches are evaluated to determine their suitability for deployment within the IT environment. They must be tested prior to their widespread deployment into the production environment to identify potential problems that could cause security or operational issues.

To evaluate and test patches appropriately, the following requirements must be followed:

1. **Patches must be assigned a risk rating to identify suitability for deployment**

Based on a review of vendor advisories, a risk rating must be allocated to each patch. This must be done in accordance with the GoS risk assessment methodology.

The risk rating applied is to be determined based on a combination of:

- The seriousness of the vulnerabilities the patch resolves; and
- The GoS's level of exposure to those vulnerabilities (relevancy).

2. **Patches must be tested thoroughly before widespread deployment**

Patches must be tested thoroughly prior to implementation into the entire production environment. This can be achieved through testing performance on:

- Non-production systems;
- Dummy computers; or
- As a last resort (and only once approved by the lead of the ICT team), a sample subset of production systems (e.g. via a pilot group), if test systems are not available.

Patches from nominated 'trusted' vendors can be immediately deployed to production without testing.

- Once provided the appropriate technical information, the CEO may designate, a software vendor as 'trusted'. A central register of 'trusted' vendors must be maintained and reviewed for suitability on an annual basis by the MCIT ICT Team.

Note: this does not mandate that all patches from a 'trusted' vendor can be deployed without testing – ideally where possible testing should still occur.

4.4 Patch Deployment

To minimise business disruptions during the deployment of patches, patches are required to be deployed in a considered and measured approach.

In order to minimise business disruptions, the following requirements are to be followed:

1. **Only patches which have been tested are to be deployed**

Only those patches which have been tested and approved for deployment must be deployed into the production environment.

The only exception to this is where a patch needs to be deployed in urgent circumstances, requirements for this is detailed further below.

2. **Patches must be deployed using established change management procedures**

Patching must be conducted using each Ministry's relevant change management procedures (in consultation with managers), including the development of rollback plans.

3. **Patches are only to be obtained and deployed from official sources**

Only patches issued by official vendors are to be applied.

4. **Patches that need to be deployed urgently must be subject to a risk-based approach to deployment**

In situations where patches cannot be tested thoroughly prior to deployment due to time constraints – e.g. because the patch needs to be deployed urgently due to a critical vulnerability - the CEO through the advice of SamCERT,must use a risk-based approach to determine what poses a greater risk to the organisation:

- An unpatched vulnerability putting the company at risk of compromise; or
- The risk of deploying a patch which has not undergone testing which could potentially impact critical business operations.

The outcome of the risk assessment and the decision taken must be recorded in the SamCERT and Ministry risk register for tracking purposes before deploying the patch (assuming deployment is considered appropriate).

5. **Patches must be deployed using automated processes where possible**

Patching must be applied without requiring end-user intervention, or disruption to business processes wherever possible (e.g. through the use of automated tools that deploy the patches after business hours).

- These timeframes should be discussed and agreed upon with system owners.

Where network components require updates but these network components do not affect the infrastructure security, updating processes may be automated after a thorough analysis of risk has been completed.

6. **Systems for which patches have not been deployed must be segregated**

Any systems which are unable, or otherwise have not, been patched or upgraded for business or operational reasons must be segregated from the rest of the IT environment.

Responsibility for identifying and segregating the IT environment lies with the ICT teams within the Ministries.

Recommended Timeframes

The following are best practice recommended timeframes for applying patches for applications[3]:

Threat Type	Timeframe
Basic	**Internet-facing services:** within two (2) weeks, or within 48 hours if an exploit exists **Commonly-targeted applications:** within one (1) month
Moderate	**Internet-facing services:** within two (2) weeks, or within 48 hours if an exploit exists **Commonly-targeted applications:** within two (2) weeks **Other applications:** within one (1) month
Advanced	**Internet-facing services:** within two (2) weeks, or within 48 hours if an exploit exists **Commonly-targeted applications:** within two (2) weeks, or 48 hours if an exploit exists **Other applications:** within one (1) month

The following are best practice recommended timeframes for applying patches for operating systems[4]:

Threat Type	Timeframe
Basic	**Internet-facing services:** within two (2) weeks, or within 48 hours if an exploit exists **Workstations, servers, network devices & other network-connected devices:** within one (1) month
Moderate	**Internet-facing services:** within two (2) weeks, or within 48 hours if an exploit exists **Workstations, servers, network devices & other network-connected devices:** within two (2) weeks
Advanced	**Internet-facing services:** within two (2) weeks, or within 48 hours if an exploit exists **Workstations, servers, network devices & other network-connected devices:** within two (2) weeks, or within 48 hours if an exploit exists

[3] Ibid
[4] Ibid

4.5 Temporary Workarounds for Addressing Vulnerabilities

There may be instances where vulnerabilities are unable to be addressed immediately with a patch. As a result, a temporary workaround may be required to address a present vulnerability.

In these instances, the following requirements must be followed to ensure that this is done securely:

1. **Interim solutions in the form of a temporary workaround must be implemented if a patch from the vendor for a vulnerability is unavailable**

If a patch is not yet available from the vendor for a vulnerability, or if testing indicates an inability to patch, the following strategies must be employed (in this order) to the best extent possible:

- Disable the vulnerable functionality within the relevant software or hardware;
- Implement segregation and isolation of the relevant software or hardware in the network;
- Restrict or block access to the vulnerable service using firewalls or other access controls; and / or
- Use virtual patching to detect suspicious traffic that may be indicative of an unpatched vulnerability on a system or application being subject to attempted exploitation.

2. **Temporary workarounds for vulnerabilities must be subject to a risk-based approach**

Decisions as to whether to implement a temporary workaround are to be risk-based and subject to approval by the CEO with advice from SamCERT and the MCIT ICT. The approvals must be recorded in the SamCERT and Ministry risk register.

The timeframe for which the temporary workaround is permitted to be in place must also be documented and reviewed prior to the expiration of that timeframe.

4.6 Patch Rollback and Contingency

Patching activities can sometimes fail, resulting in the potential for significant disruption to business processes. The most proactive way to address this risk is to develop a rollback and contingency plan prior to a patch being deployed.

The following requirements are expected to be in place to appropriately manage this phase of the lifecycle:

1. **A patch rollback and contingency plan must be developed**

A contingency plan must be developed in the event the deployment of a patch corrupts the existing production environment. The contingency plan must include backup and restore procedures along with ensuring that key staff are available when critical patches are deployed.

These plans must be approved prior to deployment by the ACEO / Manager for each Ministry's ICT division.

Appendix A – Glossary

The following glossary outlines the key terms defined in this Standard.

Term	Definition
Patch	An additional piece of code developed to address a problem in an existing piece of software.
Vulnerability	A weakness in system security requirements, design, implementation or operation that could be exploited.
Patching	The action of updating, fixing, or improving a computer program to protect the software from a vulnerability.
Patch Management Lifecycle	The Patch Management Lifecycle identifies the four broad stages that are required to be addressed to ensure the end-to-end, secure inventory, identification, testing and deployment of patches.
Temporary Workaround	A temporary workaround or measure that can be followed to reduce the risk posed by the lack of an official patch for a vulnerability. It should only be used until a permanent solution is identified or an official patch is released.
Roll Back / Contingency Plan	This type of plan enables and is aimed at returning systems and software to a last known, good state (prior to when the patch had been applied and an adverse result occurred).

Appendix B – Patch Management Strategy Per Technology

The table below is a guide that should be filled out by each ministry (for key technology assets captured in the scope of this document) within the GoS.

The purpose is to define a tailored patch management strategy and capture specific details of how patch management occurs at a per-technology level.

It is the responsibility of the ACEO of each ICT Team and or division to ensure that this patch management strategy is completed and maintained for all the business critical systems under their (and their team's) responsibility.

Technology Patching Information	Details
Vendor	<name of vendor(s)>
System criticality	< Critical, High, Medium, Low >
Patch trigger	<when is the patch applied, vendor alerts, product hot fixes, maintenance packs, etc.>
Assessment approach	<approach to how patching will be carried out specific to this type of hardware/software>
Frequency/timeframes	<how frequently is patching carried out>
Outage requirements	<does applying patch require downtime/outage, specify details>
Level of automation	<are patches applied automatically using a tool or manually, specify details>
Customer or Sensitive Data stored	<details of customer data that reside if any on this platform>

Version Management

Version	Date	Comments and Remarks
1.0		