Cyber Security Standard

Patch Management Standard

Version – V1.3

1 Overview

1.1 Introduction by the Standard Owner

Post Office is committed to protecting its employees, customers, Third Party Supply Chain and information assets from damaging or illegal actions by individuals, either knowingly or unknowingly. Post Office enables this through the development and deployment of policies, standards and guidelines which are aligned to international best practices. Effective cyber and information security is a team effort involving everyone in Post Office.

1.2 Purpose

The purpose of the Patch Management Standard is to provide a structured and consistent approach to patch management throughout the Post Office Group and to ensure that to ensure that the opportunity to exploit Post Office systems and applications is minimised by ensuring they are appropriately patched against security vulnerabilities.

1.3 Application

This policy applies to Post Office permanent employees, temporary employees, agency contractors, consultants and anyone else working on behalf of the Post Office accessing Post Office data and aligns to the requirements of the Cyber and Information Security Policy.

2 Policy Framework

2.1 Policy Framework

This standard forms part of the Cyber and Information Security Policy Set. This contains controls that form part of the Information Technology Control Framework (ITCF) governed by the overarching Post Office wide framework.

2.2 Who must comply?

Compliance with this standard is mandatory for all Post Office employees and applies wherever in the world Post Offices business is undertaken. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this standard or have their own equivalent policy/standard.

3 Scope

The following software and hardware types are in scope for patch management

In Scope
Desktops and Servers (OS only)
Business Applications (windows software)
Business Applications (non-windows software)
Firmware
Cloud based Applications and Operating Systems
End Point Security system
Mobile devices (including tablets and smartphones)
Virtual systems
Network storage systems (including Storage Area Network (SAN) and Network-Attached Storage (NAS))
Network equipment (including routers, switches, wireless access points and firewalls, IPS, IDS, FIM, WAF, Proxy System etc.)
VoIP telephony software and conferencing equipment
Networked office equipment (including network printers, photocopiers, facsimile machines, scanners and multifunction devices (MFDs))
Specialist systems (e.g., cyber-physical systems such as Internet of Things or systems that support industrial control systems (including SCADA systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC)).

If a need for patch management is identified but is not included in the above table, it is the responsibility of the system owner to make sure that they are keeping their departmental systems in compliance with this Standard. Failure to do so constitutes a violation of policy.

4 Device Management

All patches must be assessed in the context of Post Office's environment, prioritised and remediated according to business impact and criticality of the vulnerability.

The priority of patching activities will be based upon an analysis of the risk and take account of where exposure is greatest, such as with Internet and external facing systems and applications.

Only patches applicable to Post Office's environment shall be applied through a formal review and change management process.

Emergency security patches must be managed through the incident process and subject to the same review and authorisation process as routine patches.

All patches must be tested in a non-production environment before implementation in the production environment.

Systems must not directly access external networks such as the Internet for patching updates; there shall be a central internal patching system, which is used b y internal hosts for patches.

There shall be a list of applications and applicable patches and a record of those applied or not applied and the assessment upon which that decision has been made shall be maintained.

Where patches are not available, e.g. for legacy systems then compensating controls must be implemented through risk assessment performed and any residual risks managed.

4.1 Patch Classification

Vendor supplied security advisories and vulnerability patches are normally classified into different severity classifications to help identify the importance of applying the patch. The Industry Standard for classification of computer system security vulnerabilities is the "Common Vulnerability Scoring System" or 'CVSS'. Most Vendors will quote the CVSS value of each patch as it is released, to enable the security threat associated with the patch to be recognised.

Other methods for evaluating and scoring vulnerabilities are used by some vendors. These will also provide a 'Critical/High / Medium / Low' categorisation.

4.2 Incomplete Data

With some vulnerabilities, all of the information needed to create CVSS scores may not be available. This typically happens when a vendor announces a vulnerability but declines to provide certain details. In such situations, NVD analysts assign CVSS scores using a worst-case approach. Thus, if a vendor provides no details about a vulnerability, NVD will score that vulnerability as a 10.0 (the highest rating).

4.3 Patch Scheduling

Where a new applicable patch is released, the persons or team responsible for the support of the IT infrastructure will download and review the new patch to assess, according to the following:

• Emergency –	Patch will resolve an imminent threat
• Critical –	Patch will resolve a security vulnerability
• Non critical –	A standard patch release update
• Not applicable –	Not relevant

Irrespective of platform or severity classification, all patches will follow a defined process for patch deployment which includes:

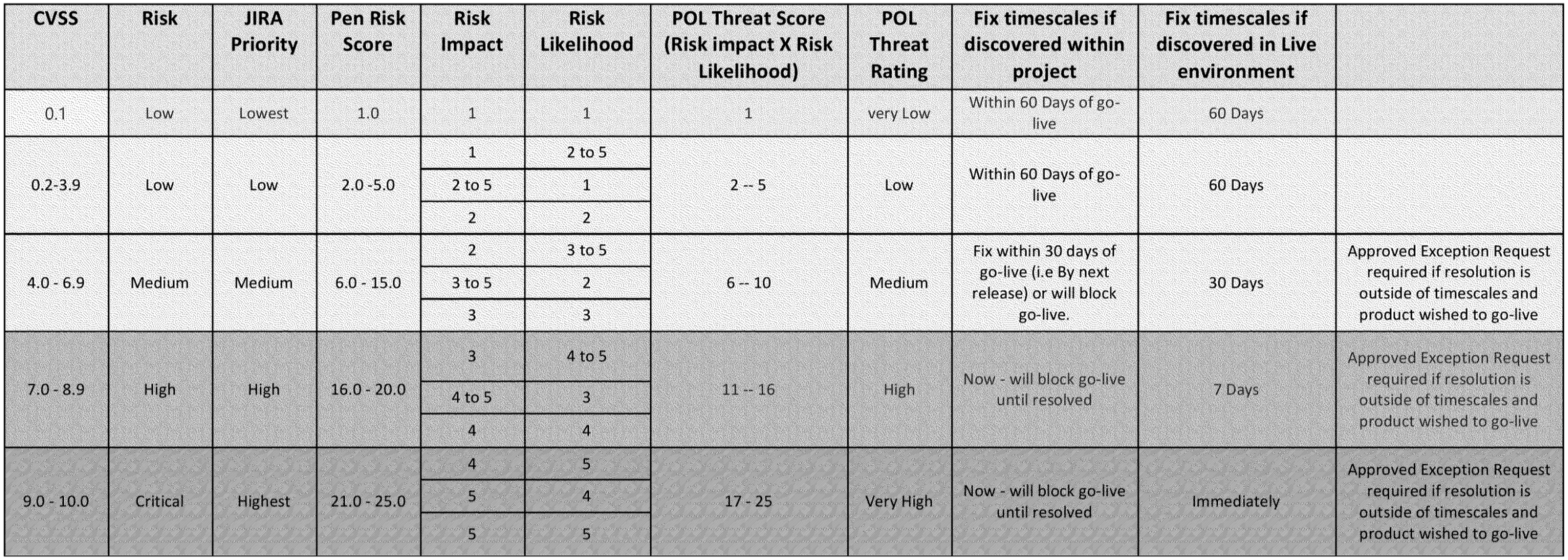
- Assessing the risk
- Testing
- Scheduling
- Installing
- Verifying

The persons or team responsible for the support of the IT infrastructure will assess the patch and examine the impact of deployment. The assessment process will establish whether the patch will cause any adverse effects. Typically, patches are to be assessed on test systems, e.g. UAT environments, before being deployed on to live environments.

4.4 Vulnerability Severity Ratings

The National Institute of Standards and Technology (NIST) maintain a National Vulnerability Database (NVD) that is a useful resource for communicating the impacts of security vulnerabilities. Many vendors now subscribe to this methodology. The NVD provides severity rankings of "Low," "Medium,", "High" and Critical in addition to the numeric CVSS scores but these qualitative rankings are simply mapped from the numeric CVSS scores:

The following table defines the criticality rating and the required remediation time:



CVSS	Risk	JIRA Priority	Pen Risk Score	Risk Impact	Risk Likelihood	POL Threat Score (Risk impact X Risk Likelihood)	POL Threat Rating	Fix timescales if discovered within project	Fix timescales if discovered in Live environment	
0.1	Low	Lowest	1.0	1	1	1	very Low	Within 60 Days of go-live	60 Days	
0.2-3.9	Low	Low	2.0 -5.0	1	2 to 5	2 -- 5	Low	Within 60 Days of go-live	60 Days	
				2 to 5	1					
				2	2					
4.0 - 6.9	Medium	Medium	6.0 - 15.0	2	3 to 5	6 -- 10	Medium	Fix within 30 days of go-live (i.e By next release) or will block go-live.	30 Days	Approved Exception Request required if resolution is outside of timescales and product wished to go-live
				3 to 5	2					
				3	3					
7.0 - 8.9	High	High	16.0 - 20.0	3	4 to 5	11 -- 16	High	Now - will block go-live until resolved	7 Days	Approved Exception Request required if resolution is outside of timescales and product wished to go-live
				4 to 5	3					
				4	4					
9.0 - 10.0	Critical	Highest	21.0 - 25.0	4	5	17 - 25	Very High	Now - will block go-live until resolved	Immediately	Approved Exception Request required if resolution is outside of timescales and product wished to go-live
				5	4					
				5	5					

When no fix available a workaround must be agreed with IT Security until a permanent fix is available and implemented.

4.5 Emergency Patching

Where patches are deemed as Emergency patches which represent a resolution to an imminent threat to the Post Office's environment, there may be a greater risk of not implementing the patch until after full testing. In such instances, the Post Office's manager responsible for IT security must be notified. An informed decision must be made based on the risk identified and a decision to deploy the patch as soon as possible or to schedule it into the next patching cycle must be made.

Critical or non-critical patches will undergo testing for each affected platform prior to deployment. The persons or team responsible for the support of the IT infrastructure will complete a validation against all images, e.g. Windows, UNIX, etc.

Operating System	Version updates to the Operating Systems	All operating systems and firmware have to be supported by a supplier that produces regular fixes for any security problems
Security	Updates to fix security weaknesses	All high-risk or critical security updates for applications (including any associated files and any plugins) installed within 7 days of release
Applications	Version updates	All applications on Post Office devices must supported by a supplier that produces regular fixes for any security problems.
HNGA - App JAVA fat client	Non-windows version updates	All applications on your devices supported by a supplier that produces regular fixes for any security problems.
HNGA - App JAVA fat client - Security updates	Non-windows software updates to fix security weaknesses	All high-risk or critical security updates for applications (including any associated files and any plugins) installed within 7 days of release

5 Where to go for help

5.1 Additional Policies and Standards

This standard is part of the Cyber Security Policy framework. The full set can be found at:

https://poluk.sharepoint.com/sites/cybersecurity2/SitePages/Cyber-and-Information-Security-Policy-Set.aspx

5.2 How to raise a concern

Any Post Office employee who suspects something is wrong has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by contacting the IT Helpdesk

5.3 Who to contact for more information

If you need further information about this standard or wish to report an issue in relation to this standard, please contact Cyber Security Team via cyber GRO

6 Version Control & Approval

6.1 Version Control

Date	Version	Updated by	Change Details
16/04/2018	0.1	IT Security	First version for comment
11/05/2018	0.2	IT Security	Updated with QSA comments
23/05/2018	0.3	IT Security	Updated post peer review
28/05/2018	1.0	IT Security	Final Approved Version
23/11/2021	1.1	Cyber Security	Updated the standard (Section 3, 4.1, 4.4 and 4.5) according to the POL Vulnerability Management Standard.
10/04/2023	1.2	Cyber Compliance	Annual update and review. Wider business input for UCF update required.
25/04/2023	1.3	Cyber Compliance	CSF approval for publication.

6.2 Standard Approval

Standard Owner:	Chief Information Security Officer
Standard Author:	Ehtsham Ali
Approved by CSF:	25/04/2023
Next review:	25/04/2024