Standard for Software Version Maintenance

Office of the Corporate Chief Information Officer & Telecommunications, Infrastructure Security Compliance

Version: 1.0

Approved by: Stephen Bull, Corporate Chief Information Officer and Sr. ADM, Office of the Corporate CIO and Telecommunications	**Owner:** Infrastructure Security Compliance Unit	
Approval date: November 17, 2020	**Last reviewed:** November 2020	**Review date:** November 2021
Contact: _GOA-ISC-Members <GOA-ISC-Members@gov.ab.ca>	**Policy Instrument type:** Standard	

Contents

Standard Statement 3
Authority 3
Scope 3
Standard Description 3
Standard Specification 3
Definitions 4
Roles and Responsibilities 4
Compliance 5
Appendix A 6

Standard Statement

This standard seeks to limit the overall exposure of government's information management technology (IMT) infrastructure and information assets to security vulnerabilities by defining an organizational approach for software update expectations. Implementing this industry standard best practice will ensure that the Government of Alberta (GoA) maintains vendor support for the software in use.

Authority

Pursuant to the Information Security Management Directive 2.3.1, equipment must be correctly maintained to enable continued confidentiality, integrity and availability of information.

Freedom of Information and Protection of Privacy Act (FOIP) Section 38 – Protection of personal information

Health Information Act (HIA) Section 60 – Duty to protect health information

Scope

This standard applies to all departments and any entity that hosts data sets and systems within the GoA IMT on premises infrastructure or cloud based infrastructure.

Standard Description

In order to minimize the number of security vulnerabilities present within the GoA's IMT infrastructure, it is critical that software running on that infrastructure is supported and regularly updated. Most software vendors will limit the number of versions of their software that they will actively support.

Outside of major version updates, it is also important that software utilizes a patch cycle as defined in the Standard Specification. Regular software patching ensures that any newly discovered security vulnerabilities are remediated in a timely manner.

Standard Specification

- Commercial off the Shelf (COTS) Software in use must either be the latest major version available from the software's vendor, or the last major version released before the current version. This specification is referred to as the n-1 requirement throughout this document.
- In all cases the software version in use must be actively supported by the vendor. If the vendor chooses not to support its n-1 version, then the only valid option is their most recent version.
- Patching cycles must be in place for software. These cycles must be run monthly, unless a service wishes to patch more often. In the case of vendors that normally release patches quarterly or longer, the patching cycle should still be prepared to run monthly in order to deal with out-of-band patches.

- Upon notification by the Director of GoA Cybersecurity of a zero day exploit, seek to immediately mitigate the vulnerability based upon advice from the GoA Cybersecurity Division and ensure that the vulnerability has been patched within 15 days of the availability of a patch from the vendor.

- Custom software that is used by the GoA, must be updated to ensure that software is not reliant on other software that does not meet the n-1 requirement.

    - For example: if a custom software runs on the Windows Operating System, that software must be updated to ensure that it will be compatible with at least the Windows n-1 version or better.

    - For example: if a custom software utilizes the Java Virtual Machine, then that software must be kept up to date in order to maintain compatibility with the Java n-1 version or better.

- Custom and COTS software that affects the ability to apply patches to other software within the monthly cycle, or the critical 15 day limit, must be updated within these same time limits to allow patching to take place.

- Wherever possible, software must utilize the automated update infrastructure provided by Client Service Management – Technology Services groups.

- It is permissible to omit patches that only provide or update features of software, as long as that omission does not result in the retention of an identified vulnerability, or prevent the software from meeting the n-1 requirement.

- A piece of software has been abandoned by a developer if there are no new versions forthcoming and no support is offered. In this situation that software can no longer remediate new critical vulnerabilities, or guarantee compatibility with the n-1 version of supporting software. A project must be initiated to find a supported replacement for this software. If it is not possible to replace the software, the situation must be identified and reported as a risk on the GoA risk register.

Definitions

- Definitions to be used in the interpretation of this policy instrument are in Appendix A.

Roles and Responsibilities

IMT Professionals (including contracted resources) will:

- Monitor version releases for software that they are responsible for.

- Initiate projects for major version updates within a timely fashion after the release of a new major version.

- Develop and maintain a patch cycle for the software that they are responsible for.

- Respond to zero day exploits as identified by the Director of GoA Cybersecurity.

Service Owners will:

- Take into consideration the service lifecycle of the software when developing a service and make allowance for ongoing support of the software when determining ongoing funding requirements.

Compliance

- Consequences of non-compliance with this standard could result in damage to Government of Alberta's reputation, expose Albertans to harm and/or incur unnecessary costs.

- Regular vulnerability scans of the GoA environment will identify services not compliant with this standard.

Appendix A

- **Criticality Level of Security Vulnerabilities**: defined by the Common Vulnerability Scoring System (CVSS) from the National Institute of Standards and Technology (NIST).
- **N-1 Requirement**: That a piece of software represents either the latest major version available from the software's vendor, or the last major version released before the current version.
- **Zero Day Exploit**: A descriptive term that highlights a critical vulnerability that the GoA Cybersecurity Director has identified as a top priority for remediation.
- **Patch Cycle**: A repeating process that tests and applies software patches to a service at a defined interval.
- **Major Version**: A software's major version will be defined by the vendor but is characterized by separate development and update releases and/or the vendor identifying differing support lifecycles for those versions.
    - For example: Apache Web Server's major versions 2.2 and 2.4 are separate major versions because they are patched separately by the vendor.
    - For example: Windows 10 Build 1803 and Windows 10 Build 1809 are separate major versions because they have defined lifecycles with differing end of life dates.