Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Patching During Change Freezes

OCTOBER 2020

Introduction

Patching operating systems and applications is an essential activity for all organisations that rely on information technology infrastructure. It is necessary for applying feature updates to operating systems and applications as well as ensuring that security vulnerabilities cannot be exploited.

Change freeze periods are typically periods of time when changes are minimised, usually to preserve business operations during critical periods. However, most organisations still allow emergency changes and patching activities during these change freeze periods via an exemption process.

This publication outlines considerations and advice in relation to patching during change freeze periods in order to enable organisations to mitigate security risks during these periods.

Patching and change freeze periods

The following considerations are applicable to all contexts when applying patches during change freeze periods.

Evolving threat landscape

In theory, the tenet of freezing almost all changes in order to preserve business operations is sound. However, in today's constantly evolving cyber threat landscape, it is important to keep in mind that new security vulnerabilities continue to be discovered by adversaries, vendors and security researchers, and that adversaries continue to operate irrespective of an organisation's self-imposed change freeze period.

The discovery of new security vulnerabilities, and disruptions from adversaries, may occur at any time. As such, organisations should ensure that security vulnerabilities are still being addressed during change freeze periods, especially within 48 hours for any internet-facing services. Critical security vulnerabilities, or security vulnerabilities that affect critical systems, should be addressed with patches or other recommended mitigations from vendors. In some cases, vendor mitigations that are not traditional patches will be provided before a patch, or alongside a patch if the patch is disruptive. Where mitigations are used, the patch should be applied as a follow-up.

Organisations can gather information about security vulnerabilities, and their associated patches and mitigations, by continuing to conduct vulnerability scans and reviewing vendor security bulletins during change freezes[1]. Initially, severity ratings from vulnerability scans will be vendor-supplied, and won't have been customised to an organisation's particular information technology environment. For example, a security vulnerability that a vulnerability scan report labels as high severity may only affect one non-critical asset that is not reachable from the internet. Similarly, a security vulnerability that a vulnerability scan report labels as moderate, such as a denial-of-service condition, may be high

[1] https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches

severity for an organisation if it affects a public or critical system. In these scenarios, the severity rating should be adjusted. In addition, vulnerability scan reports should be validated to identify any false positives.

Faults during patching

A challenge that organisations are likely to face at some point is the release of faulty patches by vendors[2] or faults encountered when applying patches to systems. This risk is also applicable outside of change freeze periods.

It is recommended that organisations account for the possibility of faults during patching in their patch management processes. Different organisations might adopt different mitigation strategies against this risk, for example, larger organisations might implement a policy of having all patches tested in a testing or staging environment, whereas smaller organisations might choose to forgo testing and mitigate the risk by implementing a rollback mechanism. Organisations using modern software environments and deployment approaches can more easily rollback their systems to a known good state. For example, some DevOps platforms enable effective 'blue green deployment'[3].

Clearly established patch management processes should be implemented in all circumstances to deal with faults during patching, regardless of whether patches are applied within or outside of change freeze periods.

Tightly coupled security and feature patches

It is always recommended that critical security patches be applied as soon as possible, and for feature updates to be applied based on an organisation's unique business needs. However, some vendors do not provide separate security and feature update patches. If an organisation does not require a new feature, being forced to apply the new feature by a vendor could introduce business process risks, as certain business processes may rely on features remaining unchanged. Additionally, having tightly coupled security and feature patches means that new features might need to be installed or supported during change freezes.

Organisations should review vendor release notes and keep up-to-date on the types of updates and security configurations that vendors provide. They should then determine if using products with tightly coupled security and feature patches is a risk. Any potential risk that has been identified may increase during change freeze periods, where possible disruptions to business operations due to feature changes is especially undesirable.

If organisations choose to use products from vendors that don't provide security-only patches, they need to account for this in their patch management processes, as they may need to be ready to implement feature changes if security vulnerabilities are high impact.

Patching and change freezes in different contexts

The following considerations are applicable for organisations that use cloud services or operate critical infrastructure.

Cloud infrastructure

Organisations that use externally-provided cloud services have a limited scope for their change freezes[4], as the technology stack and secure administration processes implemented by cloud service providers (CSPs) are often opaque. However this is unlikely to provide a significant risk, if the CSP properly patches their infrastructure and systems, as CSPs are required to provide a consistent and reliable service to their customers. For example, if an organisation freezes change at the operating system layer when using Infrastructure-as-a-Service, all their data, resources and configurations should remain the same even if the CSP performs changes underneath that layer. Similarly, if an

[2] https://www.zdnet.com/article/in-patches-we-trust-why-software-updates-have-to-get-better/
[3] https://www.redhat.com/en/topics/devops/what-is-blue-green-deployment
[4] https://www.cisecurity.org/blog/shared-responsibility-cloud-security-what-you-need-to-know/

organisation freezes change at the application layer when using Software-as-a-Service, they should not notice any difference even if the CSP migrates the application across different operating systems.

Separately, in order to flexibly and efficiently control changes for infrastructure they manage, organisations that are cloud-native might consider utilising Agile and Continuous Integration/Continuous Delivery/Deployment (CI/CD) development methodologies[5]. This allows organisations to rapidly deploy and test security patches in a controlled manner during change freezes. Moving to the cloud entails not only the transformation of technical architecture, but also the transformation of business processes.

Finally, information on the security responsibilities of CSPs and their customers can often be found via a CSP's shared responsibility model and service-level agreements. For example, organisations should note that they are still responsible for patching their operating systems and applications when using Infrastructure-as-a-Service.

Critical infrastructure

Critical infrastructure, such as Industrial Control Systems, are unique in the sense they are often in a state of change freeze due to the requirement of high availability. Organisations with critical infrastructure will most likely favour manual patching over automated patching, and find through risk assessments that it is riskier to patch than it is to withhold from patching. These organisations should still seek to apply mitigations to address any identified risks. For example, network monitoring and segmentation might be applied as a risk mitigation instead of patches. It is up to organisations to define patch management processes that are in line with their business requirements and risk profile.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.

[5] https://www.infoworld.com/article/3271126/what-is-cicd-continuous-integration-and-continuous-delivery-explained.html