Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Patching Applications and Operating Systems

First published: October 2011
Last updated: November 2023

Introduction

Applying patches to applications and operating systems is critical to ensuring the security of systems. As such, patching forms part of the Essential Eight from the *Strategies to Mitigate Cyber Security Incidents*.

In this publication, a vulnerability refers to a flaw in an application or operating system rather than a misconfiguration. Furthermore, references to patches within this publication are equally applicable to updates and other vendor mitigations.

Applying patches

Once a patch for a vulnerability is released by a vendor, it should be applied in a timeframe commensurate with an organisation's exposure to the vulnerability. For example, once a vulnerability in an online service is made public, it can be expected that malicious code will be developed by malicious actors within 48 hours, sometimes within 24 hours.

The following are recommended timeframes (in prioritised order) for applying patches:

- **Online services:** Within two weeks, or within 48 hours if identified as critical by vendors or working exploits exist.
- **Operating systems of internet-facing network devices:** Within two weeks, or within 48 hours if identified as critical by vendors or working exploits exist.
- **Operating systems of internet-facing servers:** Within two weeks, or within 48 hours if identified as critical by vendors or working exploits exist.
- **Commonly-targeted applications[1]:** Within two weeks. However, for high-threat environments, within 48 hours if identified as critical by vendors or working exploits exist.
- **Operating systems of non-internet-facing network devices:** Within one month. However, for high-threat environments, within 48 hours if identified as critical by vendors or working exploits exist.
- **Operating systems of non-internet-facing servers:** Within one month. However, for high-threat environments, within 48 hours if identified as critical by vendors or working exploits exist.

[1] Office productivity suites, web browsers and their extensions, email clients, PDF software and security software.

- **Operating systems of workstations:** Within one month. However, for high-threat environments, within 48 hours if identified as critical by vendors or working exploits exist.
- **Other applications[2]:** Within one month. However, for high-threat environments, within 48 hours if identified as critical by vendors or working exploits exist.
- **Operating system drivers:** For high-threat environments, within one month, or within 48 hours if identified as critical by vendors or working exploits exist.
- **IT equipment firmware:** For high-threat environments, within one month, or within 48 hours if identified as critical by vendors or working exploits exist.
- **OT equipment firmware:** For high-threat environments, within one month, or within 48 hours if identified as critical by vendors or working exploits exist.

Patching considerations

Identifying missing patches

One problem faced by many organisations is a lack of visibility of the true patch status of their environment. This can leave organisations unknowingly exposed to exploitation by malicious actors or otherwise thinking that patches had been applied, or reported that they had been applied, such as when they had failed to be applied successfully or were waiting on a device reboot. Using vulnerability scanners can assist organisations to gather information on missing patches in their environment. In cases where vulnerability scanners can't be used, organisations should refer to vendor documentation on how to identify patching levels and conduct manual audits instead.

The following are recommended timeframes (in prioritised order) for conducting vulnerability scans for missing patches:

- **Online services:** At least daily.
- **Operating systems of internet-facing network devices:** At least daily.
- **Operating systems of internet-facing servers:** At least daily.
- **Commonly-targeted applications:** At least weekly.
- **Operating systems of non-internet-facing network devices:** At least fortnightly.
- **Operating systems of non-internet-facing servers:** At least fortnightly.
- **Operating systems of workstations:** At least fortnightly.
- **All other applications:** At least fortnightly.
- **Operating system drivers:** For high-threat environments, at least fortnightly.
- **IT equipment firmware:** For high-threat environments, at least fortnightly.

[2] Applications on servers and workstations that are not online services or commonly-targeted user applications.

- **OT equipment firmware:** For high-threat environments, at least fortnightly.

Patching during change freeze periods

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 change freeze periods via exemption processes and procedures.

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 vulnerabilities continue to be discovered by malicious actors, vendors and security researchers, and that malicious actors continue to operate irrespective of an organisation's self-imposed change freeze period.

The discovery of new vulnerabilities, and disruptions from malicious actors, may occur at any time. As such, organisations should ensure that vulnerabilities are still being addressed during change freeze periods, especially within 48 hours for internet-facing infrastructure. Critical vulnerabilities, or vulnerabilities that affect critical applications or operating systems, should also be addressed with patches or other recommended mitigations from vendors during change freeze periods. 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 vendor mitigations are initially used, patches should be applied as a follow-up.

Faults during patching

When patching, organisations may be concerned about the risk of patches breaking applications or operating systems, and the associated outage this may cause. While this is a legitimate concern, and should be considered when deciding what actions to take in response to vulnerabilities, many vendors perform thorough testing of patches prior to their release. However, this testing is not always perfect and organisations are likely to at some point face the release of faulty patches or experience faults when attempting to apply patches to applications or operating systems.

It is recommended that organisations account for the possibility of faults during patching by establishing clear patch management processes and procedures. In doing so, organisations might adopt different strategies for managing faulty patches, for example, larger organisations might test all patches beforehand in a testing or staging environment, whereas smaller organisations might choose to forgo testing and instead implement a rollback mechanism. Organisations using modern software environments and deployment approaches can more easily rollback their applications or operating systems to a known good state.

Overall, the immediate protection afforded by patching a vulnerability that is currently being exploited by malicious actors far outweighs the impact of the unlikely occurrence of having to roll back a patch.

Tightly coupled security and feature patches

It is always recommended that security patches be applied as soon as possible. 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 risks, as certain business processes and procedures may rely on features remaining unchanged.

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 or not. 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 and procedures, as they may need to be ready to implement feature changes at short notice if vulnerabilities are being exploited and require immediate patching.

Patching in resource constrained environments

In situations where resources are constrained, organisations are encouraged to prioritise the deployment of patches. For example, patches should first be applied to internet-facing infrastructure. This should then be followed by important network devices, servers and workstations of high-risk users (e.g. senior managers and their staff; system administrators; and staff members from human resources, sales, marketing, finance and legal areas). Finally, all other network devices, servers and workstations should be patched.

Temporary workarounds

Temporary workarounds may provide the only effective protection if there are no patches available from vendors for vulnerabilities. These workarounds may be published in conjunction with, or soon after, vulnerability announcements. Temporary workarounds may include disabling the vulnerable functionality within an application or operating system, or restricting or blocking access to the vulnerable service using firewalls or other controls.

Patching in different contexts

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

Cloud infrastructure

For organisations that use externally-provided cloud services, the technology stack and secure administration processes implemented are often opaque. However, this is unlikely to provide a significant risk if the cloud service provider (CSP) properly patches their infrastructure and systems as CSPs are required to provide a consistent and reliable service to their customers.

In terms of change freeze periods, if an organisation freezes change at the operating system layer when using Infrastructure-as-a-Service, all of their data, resources and configurations should remain the same even if the CSP performs changes underneath that layer. Similarly, if an 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. This allows organisations to rapidly deploy and test patches in a controlled manner. Moving to the cloud entails not only the transformation of technical architecture, but also the transformation of business processes and procedures.

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 applications and operating systems when using Infrastructure-as-a-Service.

Critical infrastructure

Critical infrastructure, such as industrial control systems, are unique in the sense that they are often in a state of change freeze due to their requirement for 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 vulnerabilities. For example, network monitoring and segmentation might be applied instead of patching. It is up to organisations to define patch management processes and procedures that are in line with their business requirements and threat profile.

Summary

By maintaining clear and streamlined patch management processes and procedures – including an awareness of information sources used to determine whether vulnerabilities have been identified as critical by vendors or are currently being exploited, an awareness of the regular patch release schedules of vendors, defined responsibilities for individuals involved in patching activities, and regular vulnerability scanning for missing patches – organisations can position themselves to act swiftly upon vulnerability announcements and patch releases. In doing so, organisations can dramatically reduce the time between noticing information on new vulnerabilities and applying patches, or implementing temporary workarounds where appropriate.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate