



**ESSENTIAL EIGHT BEST  
PRACTICE GUIDE:  
PATCH MANAGEMENT**

# INTRODUCTION

Patch management is one of the most fundamental aspects of maintaining a good cybersecurity posture in corporate infrastructure and the end-user device environment.

However, to achieve even the first level of maturity in the ACSC Essential Eight model, businesses need to do more than install vendor-recommended patches; they must also leverage asset discovery and vulnerability scanning toolsets.

This whitepaper provides a comprehensive guide to implementing a patch management process aligned to the Essential Eight cybersecurity framework. It describes two supporting pillars of patch management—asset discovery and vulnerability scanning—then outlines nine areas for its implementation: scope, frequency, accuracy, automation, integration, remediation, communication, documentation, and compliance.

## ASSET DISCOVERY

Without knowing which assets in your environment need to be protected, it's impossible to be confident of your cybersecurity posture. Asset discovery tools perform ongoing automated scans of a corporate network to identify all connected devices. They inform the patch management process and ensure that it is aware of any new devices deployed and connected, providing a baseline of assets which must be secured by patch management.

## VULNERABILITY SCANNING

Vulnerability scanners examine some or all of the devices in an environment for missing patches, insecure configurations, outstanding vendor mitigations and various other cybersecurity risks. These automated tools maintain an up-to-date database of vulnerabilities and exploits. Best-in-class vulnerability scanners will do far more than just identify cybersecurity concerns; they will help cybersecurity teams assess and prioritise issues and provide recommended remediations.



# IMPLEMENTING EFFECTIVE PATCH MANAGEMENT



## Scope

The first step in implementing a comprehensive patch management process is to determine what set of systems and applications on the network it will cover.

To achieve maturity level one, the scope must include (at minimum) internet-facing services, office productivity suites, web browsers and their extensions, Adobe Flash Player, email clients, PDF software, and security products.

Maturity levels two and three require expanding the scope to include all applications.

To define a more inclusive scope for patch management, businesses targeting maturity level one may also leverage their business continuity plan to identify business-critical systems to add to their scope.

Risk should be the key consideration when defining the scope of patch management. For example, systems that contain sensitive data or support critical business processes should be prioritised for patch management and vulnerability scanning.



## Frequency

Once the scope of the work has been defined, the next step is to create a schedule and decide how often each of the three activities will be conducted: scanning for new assets, scanning these assets for vulnerabilities, and applying patches.

All levels of Essential Eight patch management maturity require conducting asset discovery at least fortnightly across the whole environment. However, the frequency of vulnerability scanning and patch installation may vary between systems and applications.

While scanning for vulnerabilities and especially installing patches more frequently results in an improved cybersecurity posture, this must be weighed against the increased effort, cost, and risk of disruption.

To effectively balance these conflicting elements, the frequency can be adjusted for each system and application based on its associated risk and impact of a cybersecurity incident.

Maturity level one of the Essential Eight requires vulnerability scanning to be conducted at least daily for internet-facing services and fortnightly across office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

When it comes to patch management, maturity level one requires patches, updates and vendor mitigations for security vulnerabilities in internet-facing services to be applied within two weeks of release—or within 48 hours if an exploit exists. For office productivity suites, web browsers and their extensions, email clients, PDF software, and security products, patches must be applied within one month of their release by the vendor.

For maturity level two, vulnerability scanning must be conducted weekly across office productivity suites, web browsers and their extensions, email clients, PDF software, and security products, with patches applied within two weeks of release.

Maturity level two also encompasses all other applications, and these must be scanned at least fortnightly, with patches applied within one month of release.



## Accuracy

Accuracy is a key concept in both patch management and vulnerability scanning. In the context of vulnerability scanning, it refers to how well the tool is able to identify and report on vulnerabilities. A good vulnerability scanner should also be able to provide detailed information about all of the latest vulnerabilities, including the severity, impact, and recommended remediation.

Businesses with large environments or high cybersecurity risk may implement two independent vulnerability scanning tools to reduce false positives and missed vulnerabilities. Although the cost of such a redundant setup may be significantly higher, it still may be cheaper than conducting the unnecessary manual investigations associated with false positives.

Another way to validate the accuracy of vulnerability scanning and patch management is to perform internal and external penetration testing. This helps ensure that vulnerabilities are being accurately identified, reported and resolved; however, it is not required by the Essential Eight framework.



## Automation

All effective patch management and vulnerability scanning programs leverage automation to work efficiently. This helps businesses save time and ensure consistency while reducing the risk of human error.

The Essential Eight framework requires that both asset discovery and vulnerability scanning be automated. In addition to these, however, automation can include features ranging from automatic download and installation of patches to automatic reporting of scan results.

As businesses become reliant on a wider range of software, patch management automation helps streamline the process and shield cybersecurity outcomes from the effects of resource and budget constraints.

Even level one maturity requires certain patches be installed within 48 hours. This means businesses must be constantly vigilant for new patches that affect their systems, taking action to install them immediately upon their release. Without automation, this can be a very laborious process and is unlikely to be regularly accomplished.





## Integration

Integrating patch management and vulnerability scanning into other security processes, such as incident response and risk management, helps to create a comprehensive security program in which the results of vulnerability scans are acted upon promptly.

For example, if a scan identifies a high-severity vulnerability, an incident response team can be formed, and a plan can be developed to remediate the vulnerability as soon as possible.



## Remediation

Remediation is the process of fixing or mitigating vulnerabilities that are identified during a scan. It can include applying patches, configuring systems and applications to reduce the attack surface, and implementing other security measures, such as vendor-recommended mitigations.

While the Essential Eight provides guidance on the maximum timeframe for remediation, activities within that timeframe should be guided by a well-defined security policy. This means vulnerabilities should be prioritised based on their severity and impact; those that pose the most significant risk to the business should be addressed as soon as possible,

while less critical vulnerabilities can be addressed promptly but may not require immediate action.



## Communication

Clear and quick communication is critical to the success of a patch management and vulnerability scanning program. This includes communicating with management, system administrators, and end-users about the processes and the results of scans.

For example, management should be regularly updated on noteworthy vulnerabilities identified and the progress of remediation efforts. Besides providing peace of mind, this helps make sure that patch management and vulnerability scanning processes are aligned with business objectives and that they're being implemented effectively.

System administrators and end-users should also be informed about the patch management and vulnerability scanning processes and the steps they need to take to secure their systems. This includes installing patches in a timely manner and reporting any security incidents or issues with patches that fail to install on end-user devices.







## Documentation and Reporting

Documentation in a patch management program should encompass all the aspects covered in this whitepaper—scope, frequency, accuracy, automation, integration, remediation, communication, and compliance processes.

It is also important to keep detailed records of the results of vulnerability scans and patching efforts, including which patches were applied, when, and what issues came up, if any. Detailed documentation brings consistency and efficiency to patch management and vulnerability scanning processes by providing a record of the steps taken to maintain a secure computing environment.

Management-level reporting and insights should also be produced to track the progress of remediation activities against the vulnerabilities identified and the progress of patch rollout across environments with multiple assets requiring the same patches, such as end-user devices. Reporting is especially crucial when patch installation is automated, as it helps administrators maintain oversight and ensure the toolset is working as expected.

With strong documentation and reporting, management can validate

the asset discovery, vulnerability scanning and patch management processes and be assured that the business is maintaining its targeted level of Essential Eight maturity



## Compliance

Many businesses are subject to industry regulations or standards relating to patch management and vulnerability scanning processes. These could include the Payment Card Industry Data Security Standard (PCI DSS) or ISO27001. Additionally, many cyber insurance providers require businesses to maintain and evidence their patch management process to retain their coverage.



## Decommissioning

Another essential aspect of patch management is decommissioning and removing applications that the vendor no longer supports and, therefore, cannot be patched. Maturity levels one and two of the Essential Eight framework require internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors to be removed from the environment. Maturity level three expands this to include all applications.



# CONCLUSION

Patch management, including asset discovery and vulnerability scanning, is a vital component of an effective information security program. By considering key areas such as scope, frequency, accuracy, automation, integration, remediation, communication, documentation, and compliance, businesses can implement a patch management program that greatly reduces the risk of data breaches and other security incidents.

## ESSENTIAL EIGHT PATCH MANAGEMENT AT A GLANCE

### Maturity Level One

To achieve maturity level one in patch management, businesses must have automated asset discovery and vulnerability scanning capability. Often, both capabilities are provided by a single tool.

The vulnerability database must be kept up to date with the latest vulnerabilities and exploits.

Asset discovery must be conducted at least fortnightly, and vulnerability scanning must be completed:

- Daily for internet-facing services
- Fortnightly for office productivity suites, web browsers and their extensions, email clients, PDF software, and security products

Patches, updates and vendor mitigations must be applied within:

- Two weeks for internet-facing services, or 48 hours if an exploit exists
- One month for office productivity suites, web browsers and their extensions, email clients, PDF software, and security products

All maturity levels further require all internet-

facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors to be removed.

### Maturity Level Two

For maturity level two of patch management, the frequency of vulnerability scanning must be increased to at least weekly for office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products. Patches, updates and vendor mitigations for these types of software must be applied within two weeks of release.


Finally, level two increases the scope of patch management to include all other applications, which must be scanned for vulnerabilities at least fortnightly—with patches, updates and vendor mitigations applied within one month of release.

### Maturity Level Three

Maturity level three adds the requirement to apply patches, updates and vendor mitigations to office productivity suites, web browsers and their extensions, email clients, PDF software, and security products within 48 hours if an exploit exists. It also stipulates that applications of all types must be removed once no longer supported by the vendor.



## Contact Info

 1300 348 287

 [hello@emergeit.com.au](mailto:hello@emergeit.com.au)

 [www.linkedin.com/company/emerge-it-solutions-pty-ltd](https://www.linkedin.com/company/emerge-it-solutions-pty-ltd)