

Keeping Cybersecurity Software Up-To-Date and Patched - blueAPACHE

Canonical: <https://www.blueapache.com/blog/keeping-cybersecurity-software-up-to-date-and-patched>

Details:

2024-01-15

Whilst keeping business software and particularly Cyber Security Software may seem obviously crucial, often end-users are reliant on the vendors in ensuring vulnerabilities are identified and patches rolled out.

As the Australian Cyber Security Centre (ACSC) has issued an alert about critical vulnerabilities in the Ivanti Connect Secure (ICS) VPN and the Ivanti Policy Secure (IPS) network access control solution, it is a timely reminder of practices to protect against vulnerabilities and uplift the hygiene of one's software environment.

Maintaining up-to-date and patched cybersecurity software is a fundamental aspect of a comprehensive cybersecurity strategy. It is a crucial step in safeguarding systems, data, and the overall integrity of an organisation's digital infrastructure in the face of an ever-evolving threat landscape.

Here are several reasons why running methodical software updates / patch management routines, with a best-in-class tool that helps identify these vulnerabilities, and support auto-updates with relevant documentation, is encouraged to reduce one's attack surface.

Protection Against Vulnerabilities Hygiene: Vendors constantly discover and address security vulnerabilities in their products. Updates and patches often include fixes for these vulnerabilities, making it essential to keep software current to guard against potential exploits.

Defence Against Malware and Cyber Threats: Cybercriminals are continually developing new malware and tactics. Regular updates to cybersecurity software include improvements to detection algorithms, enabling better defence against evolving threats.

Maintaining System Integrity: Security patches not only address vulnerabilities but also enhance the overall stability and integrity of software systems. Regular updates help ensure that your system functions smoothly and is less prone to crashes or other issues.

Compliance with Regulations: Many industries and organisations are subject to regulations that require them to maintain a certain level of cybersecurity. Keeping software up to date and patched is often a requirement for compliance with these regulations.

Data Protection: Updated security software provides better protection for sensitive data. By patching vulnerabilities, you reduce the risk of unauthorized access, data breaches, and potential damage to your organisation's reputation.

Prevention of Exploits and Attacks: Cybercriminals often target known vulnerabilities in outdated software. Regular updates and patches help close these security gaps, making it more difficult for attackers to exploit weaknesses in your system.

Enhanced Features and Performance: Updates may not only focus on security but also include new features and performance enhancements. Staying current ensures that you can take advantage of these improvements for a more efficient and effective cybersecurity posture.

Reducing the Attack Surface: Unpatched software increases the attack surface, providing more opportunities for cybercriminals to infiltrate systems. Regular updates help shrink the attack surface by addressing and eliminating vulnerabilities.

Proactive Cyber Security Posture Uplift: Keeping cybersecurity software up to date is a proactive approach to security. It demonstrates a commitment to staying ahead of potential threats and ensures that your organisation is better prepared for emerging cyber risks.

Is your current cybersecurity strategy keeping pace with emerging threats? Ensuring your cybersecurity software is up-to-date and patched is fundamental in safeguarding your organisation. Don't leave vulnerabilities unaddressed. Take a proactive step to reduce your digital attack surface.

If you have questions or need assistance in strengthening your cybersecurity posture, we're here to help. Reach out here for a consultation to better secure your digital environment.

why is protection against vulnerabilities important for software hygiene?

Vendors constantly discover and address security vulnerabilities in their products. Updates and patches often include fixes for these vulnerabilities, making it essential to keep software current to guard against potential exploits.

How do regular updates help defend against malware and cyber threats?

Cybercriminals are continually developing new malware and tactics, so regular updates to cybersecurity software include improvements to detection algorithms, enabling better defence against evolving threats.

What role do security patches play in maintaining system integrity?

Security patches not only address vulnerabilities but also enhance the overall stability and integrity of software systems. Regular updates help ensure that systems function smoothly and are less prone to crashes or other issues.

Why is keeping software patched relevant to regulatory compliance?

Many industries and organisations are subject to regulations that require them to maintain a certain level of cybersecurity, and keeping software up to date and patched is often a requirement for compliance with these regulations.

How does patching software help protect data?

Updated security software provides better protection for sensitive data. By patching vulnerabilities, organisations reduce the risk of unauthorized access, data breaches, and potential damage to their reputation.

What is the connection between outdated software and the attack surface?

Unpatched software increases the attack surface, providing more opportunities for cybercriminals to infiltrate systems. Regular updates help shrink the attack surface by addressing and eliminating vulnerabilities.

What contractual requirement does your Service Agreement place on customer software?

Under our Service Agreement, Customer Software must be maintained at the then current or previous release level, which is a binding contractual obligation designed to protect the organization and the

integrity of the services received.

What anti-virus requirement applies to Customer Managed Equipment under your framework?

Customer Managed Equipment must have anti-virus software installed and configured in accordance with industry best practice, and this software must be actively operated to maintain protection.

How do you deliver patch management, and what access does it require?

We deliver patch management as a proactive service through our emPOWER Managed Services framework, and patch installation requires remote access to customer systems. Approved maintenance may involve disruptive planned downtime, including reboots required by system patches.