MANAGING NON-MICROSOFT SECURITY UPDATES

Bridging the gaps left by WSUS and SCCM
Managing Non-Microsoft Security Updates

Bridging the gaps left by WSUS and SCCM

Summary
Overlooking patches for vulnerabilities on non-Microsoft® software is a growing security risk for organizations. Many businesses struggle to identify, prioritize and deploy such patches.

Objectives:
• Present the importance of patching non-Microsoft software
• Identify the challenges of patching vulnerable non-Microsoft applications
• Demonstrate how we can empower your organization to extend your processes and tools to patch non-Microsoft software

Managing Microsoft updates using Microsoft tools
Most organizations use Windows Server Update Services (WSUS) or System Center Configuration Manager (SCCM) to manage and deploy Microsoft patches to their Windows environments. The management of Microsoft patches is supported by Microsoft tools, and by their process to release updates. For that reason, most organizations do well when it comes to applying Microsoft patches.

But while patching Microsoft software is an important task, it’s not enough. Overlooking patches for non-Microsoft software is a great security risk for organizations.

Reasons to improve patch management processes
The exploitation of unpatched vulnerabilities in software remains one of the main vectors for cyberattacks, and patches are proven to be the most effective means to mitigate this security risk.

According to Secunia Research at Flexera® in the past year, while the share of non-Microsoft applications among the most popular desktop applications was 29%, they accounted for 77.5% of the vulnerabilities.

Poor patch management processes leave holes and cracks in your IT environment for hackers to exploit, leading to security incidents that can result in considerable losses for your organization. This includes business disruption, exposure of customer data, loss of intellectual property, damage to brand reputation, and all the costs associated with dealing with the consequence of security incidents.

1 Flexera Vulnerability Review 2018
2 50 most popular applications on Windows operating systems with a Personal Software Inspector installed
Understanding what hackers know

• It’s not only successful data breaches that impact organizations
  – The cost to deal with cyberattacks—associated with successful breaches or not—is, on average, US $21,000 per day.³
  – Over 60% of organizations report system downtime due to a security incident between one and 16 hours, with between 11 and 50% of the systems affected.⁴

• Old, well-known, unpatched vulnerabilities continue to be easy targets for hackers
  – Gartner predicts that through 2020, “99% of the vulnerabilities exploited will continue to be the ones known by security and IT professionals for at least one year.”⁵

• Patches are available for most vulnerabilities—you can remediate before hackers take advantage of them
  – Research shows that more than 80% of vulnerabilities have a patch available at the time they become public⁶ and that first exploitation happens, on average, 30 days after public disclosure⁷ of the vulnerability. According to the latest Flexera vulnerability review, 92.5% of the vulnerabilities in the most common applications had a patch available at the time of disclosure.

Patching the “right thing” is probably the biggest challenge when it comes to patch management processes. Knowing what non-Microsoft applications to patch at any given time is already a significant task. Knowing what to patch first is a much harder task. It is, however, the key to making patching more efficient and more effective.

Efficiency

Applications are getting patched more and more frequently, and keeping up with every patch can be challenging. By prioritizing those patches that remediate software vulnerabilities, organizations can stay secure while reducing the change management headaches of trying to address every vendor update. This approach helps free up your resources to extend the patching program, or for other key activities.

Effectiveness

Prioritizing patches according to their security risk has a significant impact on the security posture of any organization.

By applying the right patches, organizations close one of the main doors for cyberattacks, consistently reduce the attack surface for cyber-criminals and hackers, and avoid the costly consequences of incidents and breaches.

---

⁴ Cisco 2017 Annual Cybersecurity Report
⁵ Gartner Essentials: Top Security Predictions 2016
⁶ Flexera Vulnerability Review 2018
⁷ 2016 Data Breach Investigation Report, Verizon
Understanding the challenges

Improving patch management begins with an understanding of the challenges, which helps you identify solutions and address issues to achieve better results.

**Patch assessment**

Accurate discovery of vulnerable files and applications is one of the biggest challenges for patching. Most organizations have some sort of inventory data, but these tools typically rely on the add/remove programs list in the Windows registry which is often not detailed enough to accurately determine whether a device has vulnerable software.

**Patch alerts**

Many software producers fail to effectively communicate the availability of new security patches. There are exceptions, such as Microsoft and Oracle, that have regular, well-published cycles which help organizations plan and develop processes, and act when patches are released. But when dealing with hundreds of software vendors, organizations struggle to keep informed about the availability of security patches across all their vendors.

**Prioritization**

Making the distinction between security-related and functionality-related patches is already a leap in prioritization. However, the sheer number of applications deployed in organizations, and the related number of updates released every year for those applications, call for a systematic approach to determine criticality and prioritize patches. The most common approach is that vendors deem security patches “critical,” making it hard for IT security professionals to determine which ones are more important.

**Packaging and deploying**

Many popular applications have native auto update features, but this consumer feature is typically plagued with add-ons and configuration options. These need to be managed in the context of organizations due to change management processes that ensure business critical applications aren’t adversely affected by an unexpected software update.

“With SCCM, our customers can empower employee productivity on a wide range of devices while maintaining compliance and working to protect company data.

*With Software Vulnerability Manager and SCCM, our joint customers can streamline patch management processes and protect both Microsoft and non-Microsoft applications from vulnerabilities.*

Andrew Conway, Director Product Marketing, Microsoft
Flexera’s Software Vulnerability Manager provides the answer for patching non-Microsoft applications, leveraging your existing Microsoft tools and associated processes. The solution enables your team to lean on and benefit from Full Visibility of Security Patch Status for ALL Programs on your Windows Systems Map. You get visibility into your entire software inventory and can correlate this to vulnerability intelligence covering more than 20,000 programs from thousands of vendors, so you can immediately identify unpatched, vulnerable Microsoft and non-Microsoft programs.

**Understand what to patch first**
Software Vulnerability Manager provides accurate reports on the patch status for applications and systems in your environment, enabling you to prioritize with criticality ratings provided by Secunia Research vulnerability experts. You can develop and manage processes using the configuration capabilities to help further prioritize based on the risks for your own infrastructure.

**Customize packages and deploy using your Microsoft tool set**
Packages created with our Software Package System (SPS) are flexible and can be edited, with the parameters determined by you. Customizations could include:

- Updating all previous versions to the latest version
- Pre-accepting the EULA
- Withdrawing shortcuts on desktops and controlling auto update behaviors

**Summary**

**Accurate patch assessment, efficient patch management and risk mitigation**
The natural fit of Software Vulnerability Manager and WSUS/ SCCM provides many benefits for your team:

- The ability to rapidly handle and remediate non-Microsoft vulnerabilities via one console
- Optimized time and resource management
- The capacity to:
  - Pinpoint the exact vulnerabilities affecting your infrastructure
  - Simplify the patching of vulnerabilities
  - Secure your off-site assets and send email alerts upon any changes

With the right patch management capabilities in place, you’ll have a solution for the root cause of many of the security issues affecting your organization: exploitation of unpatched vulnerabilities in software.
Take charge of your patching

About Software Vulnerability Manager

Software Vulnerability Manager empowers IT operations teams to continuously identify vulnerable applications and apply security patches—before vulnerabilities that lead to costly breaches can be exploited. The solution leverages verified vulnerability intelligence and assesses more than 20,000 applications, delivering tested patch packages for non-Microsoft applications, accelerating identification of vulnerabilities, driving their prioritization and reducing time to patch.

Software Vulnerability Manager is the preferred security patching solution for more than 1,000 enterprises worldwide. They benefit from our seamless integration with Microsoft products to simplify assessment of security status and patching of critical, non-Microsoft applications.

NEXT STEPS
For more information on Software Vulnerability Manager, visit us online

ABOUT FLEXERA

Flexera helps executives succeed at what once seemed impossible: getting clarity into, and full control of, their company’s technology “black hole.” From on-premises to the cloud, Flexera helps business leaders turn IT insight into action. With a portfolio of integrated solutions that deliver unparalleled technology insights, spend optimization and agility, Flexera helps enterprises optimize their technology footprint and realize IT’s full potential to accelerate their business. For over 30 years, our 1300+ team members worldwide have been passionate about helping our more than 50,000 customers fuel business success. To learn more, visit flexera.com