Closing the Door on Cybercriminals

Best Practices for Patch Management

VIPRE®

Closing the Door on Cybercriminals

Best Practices for Patch Management

Simply put, the bad guys are constantly searching for any possible point of entry that can be exploited by viruses and malware.

It's no secret that today's security environment is more dangerous and dynamic than ever before. The sheer quantity and frequency of new threats that confronts IT professionals is daunting, as cybercriminals relentlessly probe for weaknesses and vulnerabilities in an organization's network. What's more, the rising number of end users who work remotely and/or use mobile devices makes cyberattacks on endpoints outside of the network increasingly attractive to criminals.

Simply put, the bad guys are constantly searching for any possible point of entry that can be exploited by viruses and malware. The ease and speed with which criminals now develop new threats means that virtually any application can be quickly targeted. It isn't just widely-used software solutions under attack anymore, as even relatively obscure applications and vulnerabilities are being pursued.

This heightened threat environment puts additional pressure on you to implement a comprehensive security strategy that ensures servers and endpoints don't present windows of opportunity for a security breach, no matter how temporary or seemingly innocuous those opportunities may be. Deploying a superior endpoint protection solution is obviously key, but one of the most overlooked components of an effective security strategy is patch management.

Patch management has become increasingly important because cybercriminals are constantly discovering new vulnerabilities, which forces software vendors to then respond with frequent and irregularly-scheduled patches that remove those vulnerabilities. The more quickly and efficiently you can deploy those patches, the sooner you will neutralize significant security threats.

As such, it's useful for you to review the following list of patch management best practices, which will help you formulate a cohesive patch management strategy that can maximize network security and prevent disruptions to operational efficiency and productivity.

Step 1: Develop Clearly-Defined Policies

Establishing the details of patch management policies first is crucial. This type of proactive approach enables you to evaluate potential challenges in advance and methodically determine guidelines for addressing them. By contrast, a reactive management approach is often characterized by hastily-created and poorly-coordinated ad hoc processes that lack consistency and long-term efficacy.

The fundamental objective of any patch management policy is to quickly identify and eliminate vulnerabilities. As soon as notification is received of a new patch to correct a critical weakness, the IT team should clearly understand:

- Who is responsible for administering the patch
- How the patch will deployed (e.g., manually, via automation)
- When the patch will be fully implemented
- How the patch deployment will be verified
- In what priority multiple patches will be applied

An obvious example of prioritization is to apply the most critical or important patches first. Beyond that, determining the relative urgency of deploying any given patch involves a number of factors (e.g., nature of threat a particular patch addresses, specific systems at risk for threat, etc.).

Step 2: Follow Consistent Processes

There are several ways that you can receive information about newly-released patches that address product flaws or vulnerabilities. These notifications may originate from Microsoft® Windows® Automatic Updates, the Microsoft® Security Notification Service, Remote Monitoring and Management (RMM) software, a third-party client management product, or an endpoint protection solution that incorporates patch management capabilities.

While IT professionals universally appreciate the need to prevent security holes from opening in the Windows operating system, they should not underestimate the importance of patch management for the extensive range of third-party software...

While IT professionals universally appreciate the need to prevent security holes from opening in the Windows operating system, they should not underestimate the importance of patch management for the extensive range of third-party software solutions that are deployed on desktops and servers.

Regardless of the specific tools you use to receive notifications, it is vital that you establish and follow consistent processes when implementing new patches. This will ensure you derive maximum benefit from them while minimizing any potential for conflicts or downtime. Such processes should include:

Maintaining robust network security requires constant vigilance because new vulnerabilities and patches are emerging with relentless frequency.

Evaluating Need for Patching

Periodically performing discovery to generate an accurate inventory of systems and applications running on the networks will greatly strengthen the ability to protect against security threats. You can use these reports to quickly map new patch notification information (including the patch type, rating and potentially-impacted systems) to the IT environment and determine which systems require the patch (and how quickly) to prevent a breach.

Once you've established that a patch is required, there are a number of methods to obtain the patch. Patch management tools can range from completely manual (e.g., downloading patches from the Windows Update website) to almost entirely automatic (e.g., utilizing client management software or the built-in patch automation capabilities included in some endpoint security solutions).

Testing First, Then Deploying in Stages

While it may be tempting to rush the deployment of a critically-needed patch onto the networks, it's important to note that a flawed patch can potentially wreak as much damage as the threat it seeks to prevent. Thus, testing should always be conducted before patches are widely applied across the IT environment. This caveat is particularly relevant if the network employs custom code or proprietary software to support business operations.

Even after testing has been successfully completed, it is still advisable to refrain from simultaneously applying a patch system-wide, as the testing process may have failed to identify a potential flaw or conflict. Applying patches to individual workgroups or departments enables you to closely monitor them and ensure users have retained full functionality of their machines and applications.

Verifying Installations Were Performed

Depending on the scale of a patch deployment and the degree to which it's performed manually or via automation, it's possible that the patch failed to be actually installed on some of the deployment's targeted systems. As such you should include a reporting and validation process to ensure that all of the designated systems have been successfully patched.

Step 3: Implement Automation

As noted earlier, maintaining robust network security requires constant vigilance because new vulnerabilities and patches are emerging with relentless frequency. Fortunately, solution providers are developing new processes and tools to help ease the complex challenge of keeping patch management up-to-date...and automation is one of the most powerful ways to meet that challenge.

By its very nature, patch management is an ongoing and repetitive process that lends itself particularly well to automation. Consider these essential steps that characterize patch management, each amenable to the benefits of automation:

- Periodic discovery of systems potentially at risk
- Evaluating those systems for vulnerabilities
- Downloading patches deemed necessary
- Deploying patches to systems requiring them

As a network grows, the efficiencies of automating patch management will become even more apparent as technicians are freed from performing the increasingly time-consuming (and thus increasingly costly) task of manually patching individual machines.

There are several different ways to introduce automated patch management into an IT environment:

- Client management platform with built-in patch management capabilities (either as a standalone product or part of an RMM solution)
- Third-party patching tool (e.g., Ninite, ManageEngine, etc.) to download, test and deploy updates to third-party applications
- Endpoint security solution with integrated patch management capabilities

This latter approach is especially valuable to managed service providers (MSPs), who are typically responsible for maintaining security across hundreds or even thousands of endpoints spread throughout multiple clients. The ability to control both endpoint security and patch management functionality from a single pane offers MSPs a tremendous boost in efficiency, without the significant cost or added complexity of deploying a separate third-party patching solution.

VIPRE Advanced Security with Integrated Patch Management

Recognizing that patch management is an essential component of any effective endpoint security strategy, VIPRE makes it far easier and more economical for IT professionals to actively combat viruses and other cyberthreats while minimizing vulnerability to those threats due to out-of-date third-party software.

VIPRE Advanced Security is specifically designed to meet the security needs of small-to-medium size businesses (SMBs), combining a comprehensive range of endpoint protection capabilities with exceptional ease of use via its centralized management console. Included at no charge and integrated within that console, the VIPRE Patch Management tool automatically scans each endpoint for all of the applications installed, and then collects details on the

...patch management tools included with VIPRE Advanced Security are not only vital for reducing vulnerabilities to security threats, they also boost end user productivity...

currently-installed version to see if there is a newer version available (see Figure 1).

If a new version is available, VIPRE will then locate the available version and (depending on the policy designated by the administrator) either notify the admin of this availability through the VIPRE console or automatically install the new version on the endpoint (see Figure 2).

As can be seen in Figure 3, the Patch Management functionality is easily accessible directly within VIPRE's Policy Properties pane.

It's worth noting that the patch management tools included with VIPRE Advanced Security are not only vital for reducing vulnerabilities to security threats, they also boost end user productivity by resolving software bugs and increasing application performance.

Figure 1: VIPRE automatically scans endpoint to discover all applications eligible for patching.

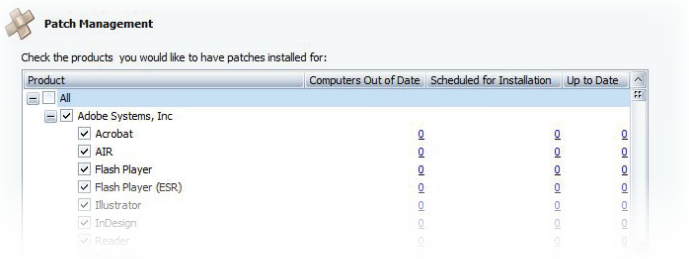


Figure 2: Patches can be individually approved for granular control.

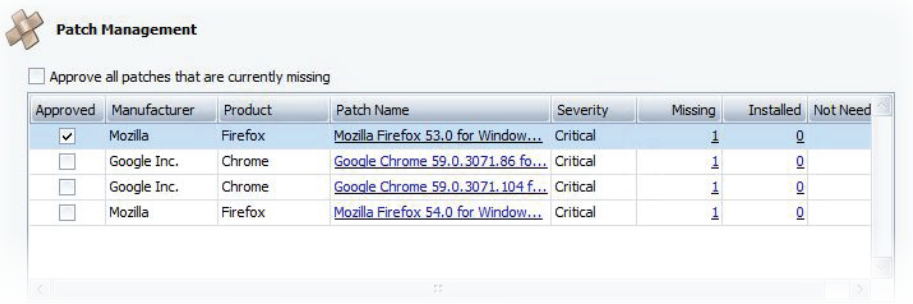
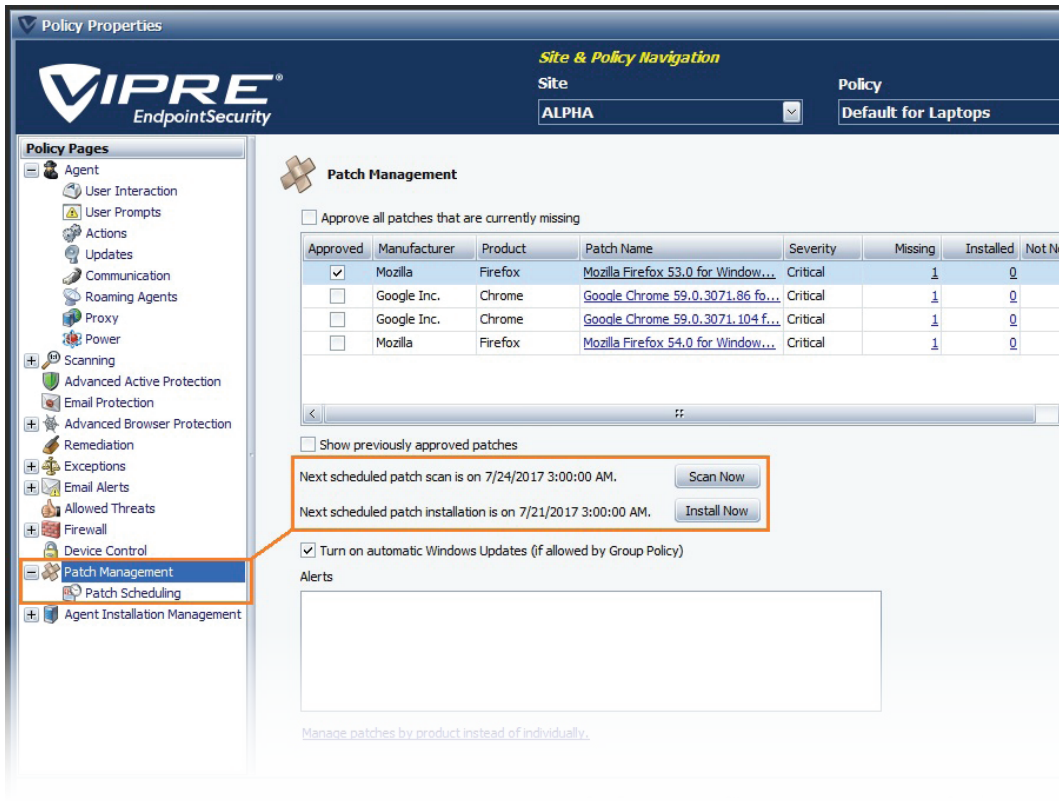


Figure 3: Patch Management is seamlessly integrated with VIPRE's management console.



Conclusion

Cybercriminals have become increasingly sophisticated in their ability to exploit vulnerabilities in the Windows operating system and third-party software. While Microsoft has implemented a broad variety of services to help IT professionals ensure they are running the latest and most secure OS software, the resources available to deploy patches for third-party software are far less accessible.

Following best practices for patch management is critical to network security, yet many third-party patch management solutions often impose high costs and can add significant complexity to IT infrastructures. An effective alternative is patch management that's integrated into the endpoint security solution, which gives you an efficient and highly economical way to ensure systems are up-to-date and protected.

About VIPRE

VIPRE is the highest-rated, award-winning internet security product for businesses and home users. It is powered by the world's most sophisticated security technologies, protecting millions of users from today's top online threats, including ransomware, zero-days and other malware that easily evades traditional antivirus. Backed by cutting-edge machine learning, one of the world's largest threat intelligence clouds and real-time behavior monitoring, VIPRE deploys in minutes to deliver unmatched protection without slowing down PCs. All VIPRE customers and partners receive free U.S.-based technical support.

C4 Computer Consulting GmbH
Vertrauen durch Erfahrung
Partnerschaftliches IT-Management

C4 Computer Consulting GmbH, visit www.c4-gmbh.de
call +49 (4106) 760600 or send email to vertrieb@c4-gmbh.de
Im Wiesengrund 3, Ellerau 25479