SOLUTION BRIEF:
THIRD-PARTY PATCH MANAGEMENT

Closing the Vulnerability Gap of Third-Party Patching

Who should read this paper

IT Managers who are trying to manage patches for third-party applications (non-Microsoft) such as Adobe, Java, Firefox, Chrome, etc.

Content

Overview

Whether you're part of your organization's security or operations team, one of your top priorities is making sure all your systems have the latest security patches in place. Maybe you have a good handle on dealing with Patch Tuesday updates, but what about all the other third-party applications and OS updates? According to SANS, "Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain."[1]

You can't afford to ignore third-party patching, but it can be an overwhelming challenge to make sure all of your at-risk third-party applications get the latest updates in a timely and efficient manner. To simplify the ongoing struggle that many organizations have with third-party patching, Symantec has developed a best practice approach that addresses all your patching concerns, including patches for both Microsoft and non-Microsoft software.

"Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain."

- SANS Institute

The 4-A Best Practice Approach to Patching

With the vast array of vulnerable applications, plug-ins, and operating systems installed in most enterprises, patch management can be an enormous time-consuming investment. Symantec's 4-A model for patch management gives you a focused, best practice approach that streamlines the process, saves time, improves coordination between the security team and operations team, and enhances the protection of your systems. The 4-A model for patch management strives to strike a balance between the concerns of the security team to address risk and the need for the operations team to manage impact and cost.

The Symantec best practice approach to effectively and efficiently patch all your applications and operating systems comprises the following four phases:

- Assessment
- Analysis
- Application
- Advancement

Assessment

The assessment phase primarily involves the security team. During this phase the security team reviews security advisories, bulletins, and threat management feeds to learn about known exploits and potential attacks on vulnerabilities relevant to their environment. They also identity the latest updates and patches that have been released by vendors since the previous rollout of updates. The security team uses this information to create a risk assessment that prioritizes the various updates applicable to their environment. Ultimately, the operations team will use this risk assessment to guide their efforts in deploying patches.

One of the biggest challenges for security teams during this phase can be identifying all the new updates that have been released by vendors. Symantec™ Patch Management Solution greatly simplifies this process by providing a report on all the patches relevant to your environment

1- SANS Institute, "Critical Control 4: Continuous Vulnerability Assessment and Remediation," Critical Controls for Effective Cyber Defense, Version 4.1 http://www.sans.org/critical-security-controls/control.php?id=4)

that vendors have made available since your last update. The report will also show you how many of your systems have already received the latest patches, how many machines those patches apply to, and how many machines still need those patches.

Once you know about the latest updates and which devices in your environment need those updates, your security team needs to create a risk assessment. As part of the risk assessment you will assign priority levels to each update to help the operations team know which updates need to be deployed immediately and which ones can be deployed at a later date.

> "According to CVE data, in 2012, the top five vendors with the most vulnerabilities were non-Microsoft vendors."[2]

In their security bulletins and advisories, many third-party vendors assign severity ratings to their updates. While these severity ratings can assist with your risk assessment, you can't rely completely on the vendors' ratings. For example, Microsoft might release a security bulletin that indicates that a certain patch for Internet Explorer is critical. However, if your organization primarily uses Chrome™ or Firefox®, and only a handful of users have Internet Explorer®, you might not consider that update as critical for your organization.

To assist with this aspect of your risk assessment, Patch Management Solution lets you define and customize your own severity levels that you can assign to updates. For example, you might define three severity levels with "1" being for those updates that apply to a vulnerability that could have a significant impact on your organization, "2" could be for patches for vulnerabilities that represent a moderate impact, and "3" might be for updates that will have a minimal impact, such as minor bug fixes or updates that don't pose a security threat.

Analysis

The analysis phase applies change management practices toward your patch and software update process. If your organization has a change management team, they will typically drive this phase. Using the risk assessment created by the security team, the change management team will define the full scope of the rollout. This includes assessing the full impact of the rollout and developing a remediation strategy. The remediation strategy needs to identify the actual updates that will be distributed, as well as which endpoints will receive the updates and which endpoints will be excluded. The remediation strategy also includes a mitigation or rollback plan that outlines steps that need to be taken if some aspect of the rollout goes wrong or creates problems.

Another key component for most best-practices is to employ predictable, orderly, and repeatable processes. This is especially true for your patch release vehicles or release schedule. You need to define standards for your release vehicles so people in your organization know when to expect the distribution of various updates. For example, you might want to use a three-tier release vehicle with each tier having responsibility for a specific severity rating, as well as being scheduled to distribute their assigned updates at a specified frequency.

The first tier might be for all updates with a severity rating of "1", which would likely need to be deployed as soon as possible after all the necessary testing has been completed. These would be considered out-of-bound releases. The second tier could be for all updates with a severity rating of "2", with these likely included in a planned once-a-month rollout that could be timed to coincide with Patch Tuesday. The monthly rollout would also include updates with a severity rating of "1" that were released as part of Patch Tuesday. The third tier would then include all updates with a severity rating of "3", which might be scheduled for deployment on a quarterly or bi-annual basis.

> "Given the sheer number of software patches, IT security and operations professionals must prioritize patching efforts to focus on those that have the biggest impact on security posture"[3]

2- http://cvedetails.com/
3- Application Control: An Essential Endpoint Security Component. Chenxi Wang and Chris Sherman, Forrester Research,Inc., September 7, 2012

In addition to defining standards for your release vehicles, it's a best-practice to prescribe phased rollouts of your patches and updates as part of your remediation strategy. Phased rollouts can minimize potential risks that might be associated with the distribution of certain patches. How phased rollouts are employed can vary from one organization to another, but a typical phased rollout starts with a distribution targeted at a small group of computers and then introduces more target computers after each successful phase of the rollout. For example, you might want to first distribute the updates to a group of test computers in a lab environment. If no problems surface with that phase you might widen the distribution to a pilot group of users in the IT organization. If you still encounter no problems, the distribution can be widened further into your production environment at whatever rate you deem appropriate.

Your remediation strategy also needs to address what to do if problems are discovered during any phase of your rollout. This could include deferring the rollout of the problematic update until the problem is resolved. If the problem only affects certain configurations of computers, you might prescribe that those computers should be excluded from the rollout until you find a solution that addresses that aspect of the problem.

In addition to a typical phased rollout, you might decide to segment the computers in your production environment into different groups, with each group having their own defined delivery vehicles. Such group segmentation might allow certain computers that are more likely to be exposed to exploits to be patched first. Some groups might be formed to accommodate system availability requirements. Others might need to take into account for system redundancy or failover processes within your infrastructure.

Application

Your operations group will be most involved with the application phase of your patch management process. Using the remediation strategy created in the analysis phase as their guide, the operations team will roll out the actual updates and patches during this phase. The main goal of this phase is to ensure that updates are deployed in a timely manner, while appropriately mitigating risk and minimizing business disruptions.

Downloading the actual update packages from vendor web sites can be one of the most time-consuming aspects of the application phase. Just as the Patch Management Solution saves the security team a considerable amount of time and effort by providing information about new patches during the analysis phase, it also assists the operations team by automatically downloading the actual update packages from vendor sites so that they can be distributed during the application phase.

To verify that all the updates and patches are successfully deployed as planned, the operations team needs to be able to produce accurate compliance reports. Compliance reports are more than just end-of-phase deliverables. Rather, they are used throughout the application phase to regularly monitor the ongoing status of the rollout. When the rollout finishes, a final compliance report can be generated as demonstrable proof that the desired compliance levels have been met. Once again, Patch Management Solution facilitates this process through its ability to automatically generate custom compliance reports throughout the application phase.

Advancement

The last phase of the 4-A best practices model for patch management is the advancement phase. During this phase all active participants involved in the other phases work together toward continuous improvement of the overall patch management process. In coordination with the different teams, they evaluate on an ongoing basis the execution of the most recent patch rollout with the goal of optimizing and fine-tuning the various aspects of each phase and the entire process. It's an opportunity to learn and benefit from past mistakes and successes.

"Much as it has in the past, the most common malware infection vector continues to be installation or injection by a remote attacker via web application vulnerabilities."[4]

Symantec Solution

Successful patch management requires an approach that goes beyond taking care of monthly Patch Tuesday updates. It requires a best-practice approach that encompasses all the third-party updates and patches relevant to your organization. It demands a solution that addresses the needs of both IT security and IT operations. Patch Management Solution delivers on all those counts.

Patch Management Solution is a best-of-breed solution modeled on industry best practices that provides comprehensive, holistic patch management for updates from a wide variety of third-party vendors such as Microsoft, Apple, Adobe, Oracle, Mozilla, Google, and many more. It offers broad coverage across Windows®, Mac®, and Linux® platforms. It automates and optimizes all phases of your patch process in a way that enables you to improve your security posture, while minimizing cost and impact on your operations.

While Patch Management Solution is available as a stand-alone offering, it is also included as part of the Symantec™ Client Management Suite. Client Management Suite enables complete lifecycle management of your heterogeneous client environments. It enables you to manage, secure, and troubleshoot your systems with greater efficiency across Windows, Mac, Linux and virtual desktop environments. Built on a scalable infrastructure with an integrated administration console, it allows you to gain and maintain control over your IT environment. Client Management Suite empowers you to achieve new levels of predictability, manage change with confidence, make smarter and faster decisions, and drive innovation for greater business success.

4- 2012 Data Breach Investigations Report, Verizon

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com