

Patch and Vulnerability Management

Aspiring To Minimum Exposure

Discovery and remediation of software vulnerabilities has become a regular task for most IT security organizations. Though there is a growing call to action for software vendors to put out more secure products by shaping up their development practices, speed to market continues to power the train and it will be some time before existing, unreasonably flawed software matriculates out of the enterprise. So for the time being, software vulnerabilities are here to stay and it is more important than ever to get a grasp on this security problem.

Patches are a means of managing vulnerabilities. For software vulnerabilities that are known and for which a patch is available, there is no better security control than applying that patch. Increasing release of patches and the inability of organizations to keep up, has caused patch management to suffer and organizations are becoming increasingly convinced that a patch management program must consist of management endorsed policy, guidelines, procedures, workflow, and accountability. It naturally follows that an efficient and effective program requires automated tools to ensure enforcement and assist in deployment.

In any given federal government agency today, you will find information security initiatives to resolve management, process, and security control deficiencies in accordance with regulations. NIST guidance, as required by FISMA, is the purveyor of the framework for security program development. Additionally, the OMB scorecard has a role in determining an agency's priorities.

NIST provides for an evolution of a security program along five levels. The final level has an agency fully integrating into daily operations, the policies and procedures that were developed during the prior four levels. It is made clear that automation is critical to this accomplishment.

This paper looks at technologies and strategies that may be used to contribute to reaching level five of the NIST guidance and achieving a state of full integration for software vulnerability and patch management.

I. The Vulnerability Management Tools Landscape

There's been a lot of chatter about the practice of "patch management" as critical to Federal Agency's information security program. Rarely do the discussions, articles, sales pitches, or even regulations, factor patch management as but only part of a more "comprehensive software vulnerability assessment and remediation program". The focus on patch management as an island is due to the velocity at which patches are being released and the accompanying pain that systems administrators experience keeping up. But there's more to it.

Many organizations also run periodic scans to discover misconfigurations, backdoors, open ports, unneeded services, and other software vulnerabilities. The scans can compare

Patch and Vulnerability Management

Aspiring To Minimum Exposure

configuration data and software patch levels with a database of known vulnerabilities and recommended remediation procedures. Pinning down vulnerabilities can be a tricky science so scanning tool vendors are distinguishing themselves with the comprehensiveness of their vulnerability signature database to accurately discover while minimizing false positives.

On the patch management front, the business of maintaining an up to date database of software patches from the leading operating system and application vendors is also a complex task. A bevy of vendors who provide this service and associated deployment management tools have cropped up to automate this burden.

Other vendors with existing products that already provide insight into the enterprise (AV, Configuration Management, etc.) also claim to “do” patch management.

Very recently, in response to marketplace demand, leading vulnerability scanner and patch management vendors have formed strategic relationships to provide total “Vulnerability Management”. Some have teamed up and/or some are providing seamless hooks into or out of their tools to accommodate this requirement and future integration with other vulnerability management mechanisms. These are a keystrides toward minimizing the gap between detection and remediation.

Because of a scanning tool’s congestive effect on a network, comprehensive vulnerability scanning is performed on a periodic basis and usually during off peak hours. Leading patch management tools, on the other hand are using “agent” technology to discover vulnerabilities. Because these agents reside on individual machines, they can explore a machine’s configuration and software information without ever leaving the local environment. This information is then packaged and sent in small footprint to the database that can return instructions to be carried out by the agent.

Additionally, agent technology used in conjunction with “relay” or “junction” servers can help to contain data flow to achieve expedience and security.

Using these techniques to acquire and deliver information, perform remediation tasks and log activity and results provides flexibility unavailable with pure scanning.

Agents, however, cannot reside on network devices such as Cisco’s IOS because of the need to recompile IOS. However, if IP range adjustments were optimized, bandwidth could be managed to enable real-time detection of devices other than servers and workstations – the bulk of the scanning target points – network disruption would be minimized.

The ideal software vulnerability management solution would have the seamless integration of vulnerability scanner, patch management, and overlaying policy and remediation workflow management and reporting tools that have integrated accountability features.

Patch and Vulnerability Management

Aspiring To Minimum Exposure

Moreover, a most effective vulnerability management tool would provide real-time understanding of an enterprise's exposure coupled with traffic monitoring and a signature database of known enumeration patterns. Unremediated vulnerabilities held against this database of exploit activity "tracks" could be used to take vulnerability management to the next level.

To date, there's no one size fits all comprehensive vulnerability and patch management solution from a single vendor (though you won't hear that from them). There are, however, tools designed to be seamlessly interoperable. When integrated, this will provide management a view of the enterprise's entire known vulnerability exposure in real time and the ability to perform remediation tasks such as those associated with effective/efficient patch management. This integrated solution will include enforcing compliance with policy and procedures using automated accountability techniques and technology.

II. NIST Security Guidance

Providing for the evolution to fully integrated security management

From NIST 800-55: "As an IT security program evolves and performance data becomes more readily available, metrics will focus on program efficiency - timeliness of security service delivery and effectiveness – operational results of security control implementation.

"IT Security Metrics...must be of maximum usefulness to ensure that available resources are primarily used to correct problems, not collect data"¹

As is a natural tendency, perhaps some federal agencies concentrate their sights on complying (with regulations) to secure, rather than securing to comply.

This is especially evident with respect to vulnerability management and patching. A review of a change management logs/documents will likely show noticeably increased activity in the month before an IG audit. The reasons for this are not usually related to neglect but to the lack of a program that includes "real-time accountability and workflow designed to ensure that patch management is integrated into the daily security routine.

Because it is reported that 80% of software exploits occur as a result of software with available but unapplied patches², patch management must be a top priority in any federal organization.

¹ NIST 800-55, Page 12, PP3

² Gartner