

Four Steps to Cure Your Patch Management Headache

Executive Summary

Using patch and vulnerability management as the principal component of your risk mitigation strategy and taking prudent measures to establish a best practices approach can help reduce costs and risks in the long term.

Overview

The need to speed up patch deployment across today's highly complex and distributed IT environment has never been more important. The heat is on to proactively safeguard your systems and endpoints from the newest exploits as the time it takes hackers to exploit a known vulnerability continues to shrink. Using patch and vulnerability management as the principal component of your risk mitigation strategy and taking prudent measures to establish a best practices approach can help reduce costs and risks in the long term.

» In the summer of 2008, it was reported that 75 percent of websites hosting malware were legitimate websites (www.pc1news.com). By the summer of 2009, the number of websites hosting malware that were legitimate sites had grown to 84 percent (www.spamfighter.com). In the first half of 2009, the number of new malicious Web links increased by 508 percent (www.bestsecuritytips.com). It's clear that simply surfing the Web has become measurably more dangerous.

» The bad guys don't need next-generation "zero-day" malware to win today. In fact, they realized long ago that we are doing a poor job of patching our systems and have taken advantage of the opportunity that these vulnerabilities present. About 71 percent of the time the vulnerabilities exploited by hackers in web borne malware are up to a year or more old, and they're less than six months old only 19 percent of the time.

» Not long ago, the time it would take the bad guys to reverse-engineer a vendor patch to create a reliable exploit was measured in weeks. Today, it is measured in hours. Many people still take between 30 and 50 days to deploy vendor patches. The reaction time, known as "time to patch," has not kept pace with aggressive hackers, leaving organizations to rely on outdated patch management and lifecycle programs and leaving their data and systems dangerously exposed.

» Obfuscation has changed the game, and our defenses are overwhelmed. The bad guys no longer need to create new instances of malware to silently pass through our defensive technologies. Today, they simply create unique instances of the same malware. Between 2008 and 2009, the number of unique instances of malware samples increased 600 percent (www.lavasoft.com).

Patch and vulnerability management continues to be the first and last line of defense against existing and newest exploits. With the sophistication and sheer volume of exploits targeting major applications and operating systems, the speed of assessment and deployment of security patches across your complex IT infrastructure is key to mitigating risks and remediating vulnerabilities. Here are four steps to cure your patch management headache.

Laying the Ground Work:

1. **Discover Assets:** Identify all firmware and software on the network and categorize them by platform, applications, department, etc.
2. **Classify Value and Risk:** Determine which systems are most critical to protect based on the assets housed and/or the function they provide. Define the level of risk by criticality of system and how prone it is to attack.
3. **Establish Workflow and Groups:** Determine ownership, permissions needed and responsibilities for threat identification, testing and remediation across security, IT and business units. Define correlating system groups.
4. **Agent Maintenance:** Ensure that all assets in the network have been fully installed with an automated patch solution. Install new patch management agents where required, if this task has not yet been fully automated with a group policy, login script or other technique.
5. **Identify Test Groups:** Build a representative sample set of each type of machine based on steps 2 and 3, in readiness for patch testing steps (11) and (14).

A Week before Patch Tuesday:

6. **Schedule Resources:** Allocate IT resources for Patch Tuesday while also integrating additional patch release schedules from Adobe, Apple (ad hoc), Oracle and so forth.
7. **Reserve Down-Time for Servers:** Reserve time slots to be able to deploy patch updates to any mission critical servers within 72 hours of the Patch Tuesday release.
8. **Watch for Pre-Announcements:** Monitor security sites for pre-announcements of patches and discussion of vulnerabilities and possible zero-day exploits that they may address from sources such as SANS, National Vulnerability Database, etc.
9. **Confirm Reporting Up-to-date:** Review and update system records of last patch deployments, and make sure all computers are being regularly scanned. Deploy any missing Service Packs, hotfixes or rollups from prior months if these are still outstanding. Remember that some patches won't install if you have missing prerequisites.

Continued »

On Patch Tuesday:

10. **Study Vendor Information:** Microsoft and other vendors provide webinars, email alerts and comprehensive online information on all new Patch Tuesday updates.
11. **Prioritize Potential Patches:** Use patch impact (Critical, Important, etc.), asset risk and value to prioritize systems for patch testing and deployment.
12. **Staged Testing:** Testing each patch is vital; automated deployment is very risky and not advised. Be certain to test the patch in each environment of your previously defined groups and deploy the patches in phases.
13. **Change Control:** Follow any internal planning and approval processes for agreeing on patch deployment.
14. **Determine Prerequisites:** Many patches are interdependent on prior updates. Check that each machine in the defined group has received the latest Service Pack or update needed.
15. **Installation of the Patches:** Stage deployments by system groups and prioritization. Start with smaller, low-risk groups, and validate that no problems occur, and then work your way to larger and higher-risk areas of the network.

After Patch Tuesday:

16. **Deployment History:** Maintain accurate records of all patches deployed.
17. **Calculate Time to Deploy:** Measure how long it takes to get all servers, desktops and laptops fully patched in your organization. This is a great metric to measure against. Remain vigilant for laptops and VPN-connected systems that may connect days (or weeks) after the initial deployment.
18. **Monitor for Compliance:** Make certain that new or rebuilt systems are “base-lined” for their appropriate systems group. Monitor for removal of patches.
19. **Checks and Balances:** If available, use a network scanner, attack scanner or secondary system to validate your system security from a different perspective. This can help identify any anomalous situations due to malware activity within your network.
20. **Metrics Improvement:** Modify system settings, distribution parameters and so forth to further optimize the system for next month's updates. WAN optimization, polling frequency and minimizing the patches being detected can all help further optimize performance. Look for computers that did not receive updates at all or those that took unusually long to receive updates.

Other Resources

- » [Reduce Your Threat Exposure Resource Center](#)
- » [Vulnerability Scanner](#)
- » [Patch Management 2.0 \(Whitepaper\)](#)
- » [Key Tips to Surviving Patch Tuesday \(Webcast\)](#)

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in operational endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Compliance and Risk Management offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Utah, Florida, Texas, Luxembourg, the United Kingdom, Germany, Ireland, Spain, France, Australia, and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Lumension, Lumension Patch and Remediation, Lumension Vulnerability Management Solution, “IT Secured. Success Optimized.”, and the Lumension logo are trademarks or registered trademarks of Lumension Security, Inc. All other trademarks are the property of their respective owners.



Global Headquarters

8660 East Hartford Drive, Suite 300

Scottsdale, AZ 85255 USA

phone: +1.888.725.7828

fax: +1.480.970.6323

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Compliance and IT Risk Management