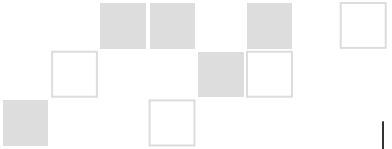


White Paper

Patch Tuesday Preparation Guide.

Patchlink Outlines Best Practices for Prioritizing, Testing and Remediating Vulnerabilities





"With PatchLink our preparation for Patch Tuesday is simple and our patching process is smooth and streamlined."

Gabriel Selmi, Network Administrator,
Advanced Behavioral Health, Inc.

PatchLink Corporation, the global leader for security patch and vulnerability management solutions, today issued comprehensive best practice guidelines to help organizations prepare for what has become a notoriously stressful IT day, Patch Tuesday.

While Patch Tuesday is often the cause of many late nights testing and applying patches, organizations face a continuous onslaught of vulnerabilities and patches that can adversely affect IT infrastructure. PatchLink's preparation guide is applicable to the full spectrum of high priority patches released throughout the month, provides recommendations for mitigating risk for vulnerabilities without patches released, and outlines best practices for remediation testing and application.

The PatchLink Patch Tuesday Preparation Guide is also available for download at <http://www.patchlink.com/redirect.asp?IDr=157&IDd=315>.

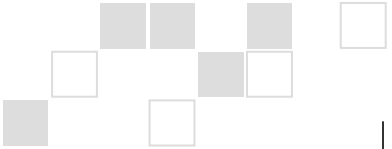
Patch Tuesday Preparation Guide

Laying the Ground Work:

1. **Discover Assets**—Identify all firmware and software on the network and categorize them by platform, department, etc.
2. **Classify Value and Risk**—Determine which systems are most critical to protect based on the assets housed and/or the function it provides. Define 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 (starting Q2 2006), 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 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.



"Prior to Patch Tuesday, we use PatchLink Update's unique fingerprinting capabilities to identify which nodes need to be updated with current patches. Once the patches are released, I research them and use PatchLink to test the patches on each station before rolling them out to the appropriate nodes."

Gabriel Selmi, Network Administrator,
Advanced Behavioral

9. **Confirm Reporting Up-to-date**—Review and update system records of last patch deployments, make sure that 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 pre-requisites.

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.
13. **Change Control**—Follow any internal planning and approval processes for agreeing on patch deployment.
14. **Determine Pre-Requisites**—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, 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 optimize the system better for next months 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 that took unusually long to receive updates.



PatchLink Corporation
Scottsdale, AZ 85255
480.970.1025

www.patchlink.com

ABOUT PATCHLINK CORPORATION

PatchLink® is the global leader for security patch and vulnerability management solutions, delivering comprehensive, multi-platform assessment and remediation for continuous protection across the enterprise. Offering the most comprehensive platform and application support, PatchLink maintains the largest tested and most up-to-date security patch repository, enabling organizations to accurately assess and remediate vulnerabilities based on established industry best practices. Currently protecting thousands of commercial and government organizations and millions of PCs and servers worldwide, PatchLink effectively eliminates vulnerability risks and enforces security and compliance policies while reducing overall IT costs.