



Managing Patches in Diverse Environments

Introduction

Organizations run on a complex combination of operating systems, applications, databases and networking platforms, any one of which can instantly expose critical data if hackers exploit a weakness in it. Each vendor faithfully rolls out patches to plug the vulnerabilities in their software, but the sheer number and variety of IT platforms makes it harder than ever to track which patches are available for which software platform; which of these patches are most critical, and to prove to auditors and regulators that the most important patches have in fact been applied.

But just as patch management has become more difficult, it has become more important. The number of attacks from hackers, the sophistication of the attacks, and the speed with which they are launched increases every year. Hackers can deploy "zero-day" attacks as soon as a vendor discloses a vulnerability, but before the vendor can release a patch. While attacks on, and patches for, Microsoft Windows get the most attention, other popular applications such as Adobe Acrobat – and open-source software such as Linux – draw more fire from hackers as more organizations rely on them for mission-critical systems. Preventing such attacks has become a top concern for CEOs and boards of directors because of stricter regulatory requirements to protect critical systems, and the negative publicity that results from lost or compromised data.

For all these reasons, IT and security administrators need a patch management solution that provides coverage for all the platforms they manage. Ideally, such a solution would provide a centralized, common infrastructure that allows them to cost-effectively gather, deploy and track the installation of the thousands of security patches released by key hardware, software and networking vendors on whom their businesses rely.

The Challenge

Hacking, once thought to be mostly the province of bored young coders looking to impress their friends, has turned into a lucrative, global criminal enterprise that grows in scope and threat every year.

Security trackers at the CERT Coordination Center at Carnegie Mellon University report that the total number of reported software vulnerabilities rose from 3,780 in 2004 to 5,990 in 2005, with another 3,997 in the first half of 2006 alone. More and more of these attacks are not aimed simply at vandalizing a Web site or proving the hackers' skill, but at stealing specific information such as customers' credit card numbers for profit. A 2005 report from security vendor McAfee Inc. said that "in the last few years, cybercrime has moved from amateurs and hackers to professional criminals."

While Microsoft Windows is still a major target because of its widespread use, hackers have noted the increasing use of other software ranging from proprietary applications to open-source software such as Linux. The spring 2006 report on top 20 Internet security vulnerabilities from The SANS Institute reported rapid growth in critical vulnerabilities including heightened attacks against the Apple Macintosh OS/X operating system as well as the open-source Firefox and Mozilla Web browsers. The National Vulnerability Database found

that 37% of vulnerabilities target popular applications other than Microsoft's, and that close to 50% of those are critical vulnerabilities.

Despite these pressing needs, as many as 95 percent of attacks are against known vulnerabilities for which patches are available. (Citing the danger that unpatched vulnerabilities could pose to critical infrastructure systems, the U.S. Department of Homeland Security in August 2006 took the unusual step of recommending Windows users immediately install a patch to prevent attackers from remotely taking control of an affected system.)

Given the complexity of gathering, evaluating, testing, deploying and auditing patches across multiple platforms, it's perhaps not surprising that so many systems go unpatched. A number of vendors have come to market with automated patch management solutions, which Gartner Inc. says "reduce the risk of outages from worm attacks and security breaches caused by the exploit of a vulnerability, by improving analysis and remediation functions. They also replace or supplement manual and slow patching processes, reducing workload while improving security posture."

However, in the same report, Gartner says the automation capabilities of such tools "are much lower for platforms such as Unix and Linux, database management systems, and networking equipment" than for Windows-based software. Clearly, a true multi-platform automated patch management solution would bring the benefits of automation to the real IT environments on which most companies rely.

Automated Patch Management Requirements

A heterogeneous patch management solution should be able to:

- Identify and prioritize the importance of all assets in the network to ensure that all potentially vulnerable systems are identified;
- Support all widely-used current and legacy operating systems and applications;
- Support the development and deployment of patches for custom, internally developed systems which can pose as great a threat as off-the-shelf software;
- Allow the prioritization of patch deployment by the criticality of the patches, the importance of the systems for which they were issued, or for specific groups of users or systems.
- Test patches to ensure they contain no new vulnerabilities and will not affect the normal operation of enterprise systems or applications. This not only reduces the workload on IT, but reduces the period in which unpatched systems are vulnerable to attack.
- Audit enterprise systems for the presence of patches, determine if patch deployment complies with corporate policies, and report on deployment activities. With more and more regulatory and legal requirements specifying how organizations must protect their data, proof of industry "best practices" is often as important as implementing those best practices in the first place.

- Provide high levels of automation and user-friendliness to maximize the effectiveness and efficiency of enterprise IT staffs. The easier the solution is to administer and manage, the more quickly the IT staff can remedy vulnerabilities and the less the enterprise must spend on patch management.

Using PatchLink Update for Complete Patch Coverage

PatchLink Update provides the most complete solution for managing and automating patch management for today's complex, heterogeneous IT environments. With the world's largest, multi-language patch repository, PatchLink provides more than 10,000 patches for the most common operating systems and more than 40 of the most common applications. This includes a wide array of Microsoft and non-Microsoft software, as well as legacy applications and older operating systems, such as Windows 98.

Operating systems covered range from the Apple Mac OS X to Hewlett-Packard HP-UX, IBM AIX, Microsoft Windows 98, Windows NT and Windows XP, Novell NetWare, Red Hat for Linux and Sun Solaris. Key application support includes Adobe Acrobat Reader, Adobe Flash Player for Internet Explorer, and the Adobe Macromedia Plug-In for Internet Explorer and Firefox as well as Citrix Systems Inc.'s ICA Win32 Client. New platform coverage also includes 64-bit Microsoft Windows operating systems, Novell SUSE, and Macintosh OS X running on Intel microprocessors.

Among the server and middleware components supported by PatchLink Update are Microsoft's .NET Framework, Microsoft Data Access Components, Microsoft DirectX and Microsoft Exchange Server. PatchLink also provides a development kit which enables organizations to write custom patches to eliminate vulnerabilities caused by flaws in internally developed applications or misconfigurations of internal systems.

For each covered platform, PatchLink Update rapidly and accurately remediates vulnerabilities and continuously monitors patches for complete network security and IT compliance. The delivery of patches is completely secured by the use of 128-bit SSL encryption, as well as through a connection secured by Verisign certificates to the customer's site. Additional RSA BSAFE Encryption provides additional security for both the transmission and storage of data.

PatchLink Update also utilizes leading-edge technology to assure that the proper patches, and only the proper patches, are deployed at all times. Its patented Digital Fingerprinting Technology™ provides a highly accurate patch and vulnerability process for automatic assessment, remediation, and continuous monitoring to ensure no systems are left open to attack. A Patch Fingerprint Profile is created for each end-point including all software, hardware, drivers, existing and missing patches for that machine. Each end point is then continually monitored to ensure that it remains properly patched and compliant with IT and regulatory policies. By ensuring that only needed patches are installed, Patch Fingerprinting also prevents "patch collisions" caused by deployment errors such as installation overwrites or re-imaging.

PatchLink In Action

Before deploying PatchLink Update, SAFE Credit Union in North Highlands, California relied on two full-time employees to manually patch 450 desktop systems scattered across 15 branch offices. That process was not only costly and time-consuming, but made it difficult to generate the detailed reports auditors demanded about the credit union's patch status. SAFE Credit Union needed a cost-effective, automated patch management solution that would work across its cross-platform infrastructure of Windows, Sun, HP-UX, Linux and Apple Macintosh platforms.

SAFE Credit Union deployed PatchLink Update in less than an hour, and now relies on only one person to deploy patches across its multiple platforms. It can also easily generate the detailed reports required by its auditors. "Given the name of our credit union, our members expect us to operate with the highest level of security," says Network Services Manager Marc Buzard. "With PatchLink Update, we are not only patching faster, but we're doing it more effectively. I now have the ability to see the patch status from a central location at any time, without having to make trips to our 15 branches. This helps ensure we are up-to-date with our patches, and also guarantees our business will continue to run smoothly."

Using home-grown script files, Senior Information Specialist Jim Cyzewski was never sure which systems at MidMichigan Medical Center had been properly patched and which hadn't. That uncertainty caused a lot of long days and unwelcome costs when the health care facility was hit by the Welchia and Nachia worms in 2003 and 2004. "We got hit with the first wave of Welchia and spent three days of hardcore worm alleviation using a removal tool and applying Microsoft patches," remembers Cyzewski. "My team had to seek out the right patches associated with these worms, and that was a lot of work, time and money in and of itself."

When Nachia hit, Cyzewski's team again "ended up running a removal tool and applying patches," he says. "I recall applying eight Microsoft patches," but even then "we were only able to patch 80 percent of our computers. We were just lucky the remaining computers never got infected."

In August and September of 2004, he evaluated several systems and patch management tools for cost and functionality and chose PatchLink Update. "Immediately, we were able to stop worrying about getting the most current virus .DAT files because PatchLink Update's mandatory baseline feature allowed us to quickly set up and manage these antivirus files along with security patches for a wide selection of operating systems and applications." Today, the IT staff rests easier -- and spends less time and money on patch management and remediation -- because PatchLink Update assures their systems are patched, and that they are kept informed of the status of those patches.

Summary

Today's network and systems administrators are faced with an unprecedented number of threats directed against a broader number and variety of systems than ever before. Their challenge is to quickly and efficiently gather, test and deploy the most urgent patches to the most critical systems, regardless of which vendor provided that server, application or operating system. Administrators need a single, enterprise-wide, multi-platform patch management solution that automates and verifies the installation of critical patches, and provides the audit trail to prove those patches meet corporate security requirements.

PatchLink Update provides these capabilities, along with asset management, ease of use, support for large enterprise deployments, greater flexibility and integration with other security solutions. It is based on one of the industry's largest repositories of patches for both current and legacy software, and provides a comprehensive platform for cross-vendor patch management. PatchLink Update is the premier automated, cross-platform vulnerability and patch management solution.

For a full list of all PatchLink support operating systems and applications, contact PatchLink Sales at 1- 800-890-6450.

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.



PatchLink Corporation
Scottsdale, AZ 85255
480.970.1025

www.patchlink.com