ITL BULLETIN FOR AUGUST 2013

ITL PUBLISHES GUIDANCE ON ENTERPRISE PATCH MANAGEMENT TECHNOLOGIES

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently published guidance on patch management technologies. Written by Murugiah Souppaya of NIST and Karen Scarfone of Scarfone Cybersecurity, NIST Special Publication 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*, is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management. The publication also provides an overview of enterprise patch management technologies and briefly discusses metrics for measuring the technologies' effectiveness and for comparing the relative importance of patches.

Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are important because they mitigate software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Patches can also add new features to software and firmware, including security capabilities.

The new publication examines the challenges inherent in performing patch management and emphasizes that organizations which do not overcome these challenges will be unable to patch systems effectively and efficiently, leading to compromises that were easily preventable. All organizations should carefully consider patch management in the context of security because patch management is so important to achieving and maintaining sound security.

To improve the effectiveness and efficiency of their enterprise patch management technologies, organizations should implement the following recommendations:

Organizations should deploy enterprise patch management tools using a phased approach.

This approach allows process and user communication issues to be addressed with a small group before deploying the patch application universally. Most organizations deploy patch management tools first to standardized desktop systems and single-platform server farms of similarly configured servers. Once this has been accomplished, organizations should address the more difficult issue of integrating multiplatform environments, nonstandard desktop systems, legacy computers, and computers with unusual configurations. Organizations may need to use manual methods for operating systems and applications not supported by automated patching tools, as well as for some computers with unusual configurations.

Organizations should reduce the risks associated with enterprise patch management tools through the application of standard security techniques that should be used when deploying any enterprise-wide application.

Deploying enterprise patch management tools within an enterprise can create additional security risks for an organization; however, organizations that do not effectively patch their systems face a much greater risk. Such tools usually increase security far more than they decrease security, especially when the tools contain built-in security measures to protect against security risks and threats. Risk associated with these tools include patches being altered, credentials being misused, vulnerabilities in the tools being exploited, and entities monitoring tool communications to identify vulnerabilities. Examples of possible countermeasures to these risks include keeping the patching solution components tightly secured and up-to-date, encrypting network communications, verifying the integrity of patches before installing them, and testing patches before deployment.

Organizations should balance their security needs with their needs for usability and availability.

In addition to addressing security needs, organizations need to consider the usability and availability of their information assets. Examples include:

- Installing a patch may "break" other applications; this can best be addressed by testing patches before deployment;
- Forcing application restarts, operating system reboots, and other host state changes is disruptive and could cause loss of data or services; and
- When acquiring updates over low-bandwidth or metered connections, it may be technically or financially infeasible to download large patches over such connections. Organizations should make provisions for ensuring that their enterprise patching solution works for mobile hosts and other hosts used on low-bandwidth or metered networks.

In conclusion, organizations need to balance the need to apply patches with the need to support IT operations. NIST SP 800-40 Revision 3 provides detailed information on the benefits and challenges of patch management in the enterprise.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email elizabeth.lennon@nist.gov

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.