Global Information Assurance Certification Paper

Keeping Current with Patches

David C. Vogel GSEC certification, version 1.4b, Option 1

Abstract

Administrators today face a daunting task of keeping their installations secure. While firewalls and anti-virus products are necessary to keep intruders at bay, proper patch management is just as important. At this time, keeping current with patches requires a large amount of manual effort. Provided within this document are steps an administrator may adopt to maintain site security through patch management.

Problem

Aberdeen Group "estimates enterprises worldwide currently spend over $2 billion annually to investigate, prioritize, and deploy patches for security vulnerabilities."[1] The numbers of vulnerabilities and their complexity are increasing at an alarming rate. This increase can be attributed to a number of factors. Some argue that vendors are pushing buggy, un-tested products out the door, relying on customers to perform field-testing and fault identification. Others believe the complex nature of today's applications do not allow testing to occur in a typical manner. Yet another segment thinks security is not a design criteria when the product is in its initial stages of development – security is seen as an afterthought – applied at product release. Whatever the view, the problem remains the same. Identifying, testing and resolving these problems is frustrating, time consuming and seemingly never ending.

Lance Spitzner, coordinator of the Honeynet Project, believes patching is one of "the top two things an admin can do to secure their computers"[2]. The other is turning off unnecessary services. While the patches are published and released to the public, they are not always installed. This can be attributed to lack of knowledge and training by some administrators but also due to a lack of time. Some harried administrators spend hours searching vendor and security websites looking for the latest vulnerabilities and patches. If they are lucky, no applicable vulnerabilities for their site will be found. On the other hand, if problems are found, the next several hours, and possibly days, are spent researching, testing and installing the appropriate fixes. Aberdeen indicates that gathering and installing the patches account to less than half the cost of dealing with the actual patches. More time is spent on research rather than on the actual installation of the patches.[1] Unfortunately, the standard method for identifying, researching and resolving these problems today is still a manual task. Several vendors, in an attempt to lessen the amount of time and effort to solve the problem, have created tools and services to automate vulnerability notification, patch delivery and installation.

Patches are released not only to resolve security problems but also to fix operational issues and ensure smooth running systems. Whether labeled as a patch, hotfix, update or upgrade, they have in common a need to resolve a problem. Potentially, all devices on your network may require patches at some point in time. Firewalls, routers, print sharing devices, and PDAs must be included to the list of servers, desktops and laptops. If security updates and fixes are not installed, the consequences can be monumental. Many reports of break-ins and compromises occur in the news media almost daily and list the targeted company. This is not the type of publicity a company wants. Perhaps more damaging than the credibility factor is the loss or modification of private data, which can result in loss of business and potential lawsuits by customers or clients. Time is also wasted in responding to a security breach. Users suffer downtime, loss of productivity and in many cases, substantial time and effort are spent rebuilding, reloading, and restoring systems and applying patches that, if installed in the first place, could have prevented the problem.

Staying up to date with vulnerabilities, exploits and patches has been, and continues to be a manual exercise. Along with being extremely time consuming, the manual approach to patch management has some serious problems. One, is the issue of missing an important problem or update. Another, is the inability to apply the appropriate fix due to a lack of time or labor resources.

Listed below are some steps an administrator should consider to keep an installation current on patches and up to date on vulnerabilities. In time, the steps may become automated through the use of a commercial product or service. Whether the manual or automated method is used, raising the visibility and knowledge of patches increases the security of the organization.

Staying Current

Inventory

To effectively manage site security, it is imperative to know what products are in use by the organization. The first step would be to perform a site audit. Readily available inventory tools – some free – will produce a list of operating systems, products and applications in use. Depending on the tool used, detailed hardware information can be gathered on the installed systems. Some tools allow the surveying application to run remotely, but it may be best to visit each system and look for potential problems such as modem connections with remote control software or rogue wireless access points. The survey must include all the systems onsite as well as laptops of traveling users and systems of remote workers. Potentially, each product and application in use will require some type of patch or modification to improve security. The number of unique products multiplies the amount of time necessary to identify, research and resolve problems. It therefore behooves an organization to limit the number of products

and applications. Many times individuals or departments have the flexibility to acquire and install products without IT involvement. Many times these installations are performed with default settings that are not necessarily the most secure.

When reviewing the results of the audits, you may be surprised at the number of products (and perhaps systems) you knew nothing about. This is also a good time to present the audit findings to management and discuss the dangers of de-centralized purchases and acquisition and installation without involvement by technical staff.

Vulnerability Scanning

Once the audit is complete, a vulnerability scan of the network is in order. Vulnerability scanners probe other devices to discover security holes. Network vulnerability scanners generally comprise of a scan engine, a vulnerability database, a results database, and an administrative console.[6]

Depending on the scanner selected, detection of some operating systems and applications may not be included. Therefore, it is a good idea to compare the results of the audit information with the results of the vulnerability scanner. It is also important to select the vulnerability scanner based on the products used on your site.

The results of the scan serve as a snapshot of the systems, applications and with some scanners, the services in use or registry settings. Only by ensuring the latest version and databases of the selected scanner are in use can an administrator detect the latest vulnerability known and detectable by that particular scanner. Commercial scanners include ISS' Internet Scanner and Symantec's NetRecon. An example of an open Source scanner is Nessus.

Monitor websites and lists

Upon determining the mix of products and applications in use, a visit to the various vendors' website is in order. Most have security pages containing details of known problems along with descriptions and details of fixes. Many vendors also have mailing lists with automated notifications of announcements of alerts and resolutions.
Subscribing to mailing lists and updates from security sites offers a different and necessary perspective. Many of these security sites are independent of vendor influence and in some cases, force vendors to address identified problems. It is a good idea to set up a separate e-mail account to receive these messages or to have them delivered to a shared folder. Depending on the number of subscribed sites, the amount of e-mails may be substantial.

The release of vulnerability information varies from site to site. In some cases, the vendor's site is the last to publish any information on the problem and may downplay its severity. The explanation of the timing differences partially depends on which entity discovers the vulnerability. Discovery may be made by a black-hat, security researcher or the vendor. Each may have different motives for disclosure. The black-hat – for exploitation, the security researcher – in some cases for recognition, the vendor – for maintaining the product.

There are several initiatives to assist in the timing of vulnerability releases. One is called the "Responsible Disclosure Model"[7] whereby the vendor is presented with the details of the problem and nature of the attack. If the vendor does not respond and publish a resolution within a specified time period, the researcher will publish the information on the appropriate public forum.

Sources for Vulnerability and Patch Details

When viewing vulnerability, a CVE, ICAT, CERT, or BugTraq entry may be present. Most of the vulnerability scanners contain and will list identified vulnerabilities by the CVE entry. Different entities maintain these lists. CVE is maintained by MITRE, ICAT by the National Institute of Standards and Technology, CERT/CC through Carnegie Mellon University and BugTraq by SecurityFocus.

"CVE (Common Vulnerabilities and Exposures) is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures".[8] While definitions for both 'vulnerability' and 'exposure' may vary, the intent for the CVE list is to share information among manufacturers, vendors of vulnerability managers, researchers and administrators. Vulnerability products are updated with CVE entries and use the information to develop a method to scan for the problem.

ICAT metabase is a "searchable index of computer vulnerabilities"[9]. ICAT not only lists the vulnerabilities according to the CVE naming conventions, but also provides links to a variety of public databases and patch sites. Searches can be constructed by using over 40 attributes including combinations of vendor name, CVE entry, software name and version number. One way the ICAT may help an administrator is in their severity ranking of vulnerabilities. Vulnerabilities can have a severity rating of either High, Medium or Low.

CERT/CC publishes its Vulnerability Notes database as well as Advisories. CERT/CC ranks the severity of vulnerabilities into five different categories: "advisories, current activity, incident notes, vulnerability notes, and tech tips"[10]. Advisories have the highest ranking and, according to CERT/CC, those with the most serious consequences and requiring immediate action.

BugTraq is another valuable source of information to the administrator. Maintained by SecurityFocus (now part of Symantec Corp.), BugTraq maintains a moderated mailing list and archive detailing vulnerabilities, examples of exploits, and sources of patches and fixes. BugTraq differs from other sites in that there is an open discussion regarding problems, exploits and fixes. The philosophy is that of open disclosure whereby details of vulnerabilities are disclosed for review by all parties. While this philosophy brings details to those trying to solve the problem, it also brings the same information to those bent on exploiting the problem.

Patch now, or later?

Once a vulnerability has been identified, it must be evaluated for its applicability. If the vulnerability exists within an organization, a patch or fix must be located. Most experts agree that patches should only be applied if the symptoms and conditions are met. If, for example, a site isn't running Microsoft's IIS, there is no need to apply a series of patches addressing IIS' problems. On the other hand, if you are running IIS, it must be determined if your configuration is at risk. If you are simply running IIS on an Intranet it may not be affected. Each patch should have a "Read me" file listing the overview and changes to be made and files to be replaced. It is important to pay attention to this file and not skip over it.

Determining the risk factor and priority is an inexact science. Experts, analysts and researchers may designate a vulnerability as only a minor threat, but no one understands the environment as well as the knowledgeable administrator. If you think a problem has a higher priority then adjust the priority, document the reasoning and schedule a patch session.

It is helpful to ask a series of questions when determining risk and patch priority.

- How difficult is the vulnerability to exploit, how likely is it to occur?
- Are there confirmed instances where the attack has been successfully implemented?
- If your site was compromised, what may be lost, stolen or modified?
- If this were to happen, what is the effect of downtime, reloading and rebuilding?
- If compromised, what's the cost of business goodwill and negative publicity?

Again, it is helpful to monitor some of the sites frequented by fellow admins and assess the severity of the problem. Peers within the same industry or those running similar configurations may be a sounding board and a good source of knowledge. Application vendors usually have moderated user groups and allow customers to subscribe to share information.

Documenting the patch as you wade through the information will save time in the long run. Detail the vulnerability identification (CVE, CERT, ICAT, BugTraq id, vendor id), problem, symptoms, urls for patches, comments, and a space to list

follow up tasks or difficulties encountered during or after application of the patch. A quick update to management may be in order. Give a brief, non-technical, description of the vulnerability, the applicability, the fix, and the plan. If you determine the patch can wait, let management know. Management may also help determine the priority and offer suggestions as to the best time to bring applications and or servers down for maintenance. If a test server or system is available, apply the fix and test the affected system or application.

Plan ahead

A good rule to live by is – expect the unexpected. Nearly everyone has been in situations where a quick fix and a quick reboot is all that's needed to resolve a problem. Something goes astray, several hours have passed and backup tapes have been mounted for a restore. By all means, have a tested verified backup in place just in case the unthinkable happens. Before applying patches, if feasible, create a backup of the days changes or of mission critical files.

The patch documentation lists the files or modifications made to the system. Make sure there is adequate disk space for the files and also for the uninstall or rollback procedure. Occasionally, an update can cause problems or affect other applications or services. Key application vendors should be contacted to determine if there are any issues with the patch in question.

With every scheduled patch session, a bailout plan is in order. A good plan will establish timeframes and milestones. Consider the window of opportunity to have systems unavailable and act accordingly. Ensure you have a recent copy of emergency repair or boot disks and also a fresh set of diskettes or CD to make new ones after the patch or patches have been applied and tested. Copy the patch along with your notes and documentation and place on a CD. By placing this with the distribution media, all relevant patches and fixes are in the same location and can be applied quickly in the event a rebuild is necessary in the future. Be aware that some fixes you apply may be contained in future releases of updates, service packs or product enhancements.

Tools

Vendors are aware of many of the issues and problems facing administrators today. Microsoft, for example, has provided some tools to make the life of an administrator easier. MBSA (Microsoft Baseline Security Analyzer) has a GUI interface and scans one or more systems and looks for common security risks. Alerts will be generated for items such as insecure registry settings, accounts having blank or weak passwords, and misconfigured zone settings within Outlook or Internet Explorer. MBSA will also determine if all relevant security hotfixes have been installed. If several hotfixes are missing, the output can be used to create a to-do list for installations.

The scanning mechanism for MBSA is HFNetChk. HFNetChk was written by Shavlik Technologies and checks for the patch status on supported systems. Both MBSA and HFNetChk rely and require the most current XML security hotfix database downloaded from Microsoft.

In addition to the tasks performed by Microsoft's HFNetChk and MBSA, Shavlik Technologies products have the ability to schedule and deploy patches throughout the environment. Another valuable feature is the option of scanning by product, machine type or patch identity. By narrowing the candidates for appropriate patches, time is saved both in scanning and reviewing the scan reports.

Microsoft has also created a utility called Q-chain that enables several hotfixes to be applied at the same time. This can be a great time saver by eliminating a reboot after applying each individual patch. Q-Chain also has the ability to put hotfixes in the correct order. Some fixes have dependencies and must be applied in a specific order. Before Q-chain, it was possible to apply patches individually and in the wrong order. Files intended to be updated could be overwritten by the earlier patch. By adding flags to Qchain, reboots can be suppressed, log files with paths created, and with utilities from Microsoft's Resource kit, a logoff, shutdown and reboot can be performed.

SUS is a new utility released by Microsoft that essentially replaces Windows Update on Windows 2000 and Windows XP systems. Older systems such as Window 98 and Windows NT are not supported by SUS and must rely on the older Windows Update. Windows Update only runs on a single computer and can be time consuming to visit each system in your network. SUS addresses and solves some of these problems by implementing scheduling and push technologies.

SUS is comprised of both server and client components. The server component must be installed on a Windows 2000 server that is not a domain controller. SUS can download copies of Windows updates and schedule times to check for new updates. One feature SUS has is the ability for the administrator to evaluate fixes on test systems then approving updates for affected systems. Updates may only be installed on a client if they have been approved by the SUS manager.

Automated Commercial Tools

Many of the manual steps and processes necessary in keeping systems current have been implemented in commercial tools and services. For smaller sites, cost constraints may rule these products out but, if an administrator tracks the time spent on identifying, researching and implementing patches and fixes, the overall expense of these automated products may be a bargain. If the tools and services are able to perform these time consuming tasks, the administrator's efforts may be spent on other proactive projects.

It is important not to be lulled into a false sense of security with any automated tool. Some steps, such as research and identification are performed by the tool or service but others, such as prioritization and timing should be made internally. Administrators still need to review and test the patches, then sign off on implementation. Vendor and security focused websites still need to be visited to gain additional knowledge on current exploits and patches.

Most automated tools either inventory the systems or use the output from open source or commercial vulnerability scanners. UpdateEXPERT from St. Bernard Software is one example of a commercial tool automating the chore of keeping Windows systems and Microsoft applications current. From a console, an administrator can read about an update sent by St. Bernard, query the systems for applicability, deploy to the affected systems and validate the installation. UpdateEXPERT can also schedule visits to St. Bernard's site to retrieve new patches along with other relevant site and system information.

When evaluating any tool or service, ensure support for your product mix. Several of the products support only current Microsoft products. If a site has older Microsoft products in use or has Linux, Unix or proprietary systems, the choices of tools may be limited. Consider the following when evaluating the various products and services.

Shop around – ask questions – read the documentation
Ask for a demo of the product within your environment
Get references from similar sites with similar product mix
Are agents required to be loaded on systems?
Are dedicated systems necesseary for patch and information repositories?
Ask about encryption of data to and from sites
Does the vendor store any of your inventory or status information on its site?
Does the product require any firewall modifications to work properly?
How does the product work over your corporate network?
Can the product support remote sites and workers through VPNs?

The Future

Automation and information sharing is the key to patch management in the future. Today, there are several products in existance but few, it seems, that meets the needs of an enterprise with a mix of operating systems, applications and products from a variety of vendors. Administrators are still required to visit multiple websites or wade through a myriad of e-mail messages to find vulnerabilities and potential fixes. MITRE's CVE, NIST's ICAT, CERT/CC's Vulnerabilitiy Notes Database, vendors security and update websites all have unique naming conventions and formats. A common schema must be agreed upon to simplify the process of vulnerability assessment and patch remediation.

Links must also be provided between these databases with one field serving as a key field.

MITRE's concept may be the best example of cooperation and data sharing and

graphic Ref. 17

may serve as the template for vendors, researchers and government agencies to follow.

Several partnerships have been and are being formed between vendors, government and research entities. As an example, St. Bernard Software has an agreement with Tally Systems to provide WEBCensus PC inventory service and also with ISS to provide a patch management and remediation tool along with an intrusion protection solution. The purpose of these partnerships is to complement the products and services each vendor provides. With time, these partnerships will grow and formats will be agreed upon to share information and provide products, services and solutions to provide vulnerability assessment, patch management and remediation.

Conclusion

Steps to keep an organization current on patches have been presented. The number and complexity of exploits is increasing with no end in sight. The administrator must create and follow procedures to keep an installation current on patches, fixes and updates. These steps require a significant amount of time and effort. In time, affordable products and services will automate a large amount of these tasks and free the administrator to perform more productive functions.

References:

[1] Hemmendinger, Eric. “Automating Security Patches for the Enterprise: a Two-Billion-Dollar Business Opportunity.” Aberdeen Group Insight, June 10, 2002
[2] Lemos, Robert. “Patchwork Security”. January 24, 2001.
URL: http://news.cnet.com/2009-1017-251407.html?legacy=cnet&tag=prntfr
[3] Collett, Stacy. “Manage Those Patches.” July 15, 2002.
URL: http://www.computerworld.com/securitytopics/security/story/0,10801,72647,00.html
[4] Martin, Robert A. “Managing Vulnerabilities in Networked Systems” November 2001, URL: http://cve.mitre.org/docs/CVEarticleIEEEcomputer.pdf
[5] “Keep operating systems and applications software up to date”. April 2001,
URL: http://www.cert.org/security-improvement/practices/p067.html
[6] Iwanski, Tom. “Network Vulnerability Scanners.”, Windows and .NET Magazine, March 2002 (2002) :53-57
[7] Morgenstern, Michael. Parker, Tom. Hardy, Scott. “It’s Time to be Responsible” March 1, 2002. URL: http://online.securityfocus.com/guest/10711
[8] “The Key to Information Sharing”.
URL: http://www.cve.mitre.org/docs/docs2000/key_to_info_shar.pdf
[9] “ICAT Metabase Documentation”.
URL: http://icat.nist.gov/icat_documentation.htm
[10] “Welcome to the CERT/CC Vulnerability Notes Database”.
URL: http://www.kb.cert.org/vuls/
[11] “BugTraq Frequently Asked Questions”.
URL: http://www.securityfocus.com/popups/forums/bugtraq/faq.shtml
[12] Niser, Paul. “Managing Security Hotfixes.” Windows and .NET Magazine, July 2002 (2002) :33-36
[13] Wettern, Joern, Ph.D. “Keeping Windows Current – Part One.”
URL:
http://infocenter.cramsession.com/techlibrary/GetHtml.asp?ID=1675&GetDes=&CatID=229
[14] Wettern, Joern, Ph.D. “Keeping Windows Current – Part Three.”
URL:
http://infocenter.cramsession.com/TechLibrary/GetHtml.asp?ID=1749&GetDes=&CatID=405
[15] “The Full Version of Microsoft’s HFNetChk.”
URL: http://www.shavlik.com/security/prod_hf.asp
[16] “Scan and Patch Security Holes With UpdateEXPERT.”
URL: http://www.stbernard.com/products/targetpages/winsa1-ue.asp
[17] Martin, Robert. Christey, Steven. Baker, David. “A Progress Report on the CVE Initiative.” The MITRE Corporation.
URL: http://www.cve.mitre.org/docs/docs2002/prog-rpt_06-02/CVE_FIRST_paper.pdf
[18] “St. Bernard Software Teams with Internet Security Systems to Deliver Internet Security Protection and Remediation Solution.” July 17, 2002
URL: http://www.stbernard.com/press_releases/2002_iss.pdf
[19] “St. Bernard Software’s UpdateEXPERT and Tally Systems’ WebCensus to Help IT Managers Improve Software Management and Productivity.” June 5, 2002
URL: http://www.stbernard.com/press_releases/2002_tallysys.pdf

Links:

ISS' Internet Scanner
http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php
Symantec's NetRecon.
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46&PID=13173435&EID=0
Nessus
http://www.nessus.org

---

g