Global Information Assurance Certification Paper

Patch Management – Best Practices

Wai Lee Chan
GIAC Security Essential Certification (GSEC)
Practical Assignment 1.4b (August 2002)
GSEC Practical Option 1
Submitted on: June 9, 2003
Wai_Lee_Chan_GSEC.doc

Table of Contents

ABSTRACT

In Information Technology (IT) industry, a patch is a computer program used to correct programming errors of an original program. Patch management is an orderly deployment of patches and fixes to computer systems. In recent years, due to the Internet, computer systems are visible to the public. Patch management becomes a counter-measure to the Internet threats. The security environment requires that an organisation to be good at patch management. This paper discusses some best practices of patch management. The adoption of these best practices will relieve system administrators from recurring tension of rushing patches to production systems and enable them to expedite patch management effectively.

INTRODUCTION

Operation systems and applications are computer programs that are written by many different programmers. The phrase "To err is human" effectively states that computer programs created by human beings have errors. Estimates indicate around five to fifteen "bugs" for every thousand lines of program codes.[1] Some of these "bugs" do not cause any issues while others could produce undesirable effects on functionality, performance, stability, integrity or even the security state of the of system. To correct errors of the computer programs, software companies release another program that "fixes" or "patches" the program to correct coding errors. Patch management is a process of managing orderly deployment of fixes or patches to computing systems. It has always been the method which IT professionals correct weaknesses of computer systems since the invention of computers. In recent years, due to the popularity of the Internet, computer systems are visible to the public. Criminals make use of these programming "bugs" to exploit systems in Cyberspace to gain their benefit. Patch management becomes an important layer of integrating security. Today, businesses in the United States of America spend roughly two billion dollars a year on patch management.[2]

Table 1 below illustrates six well-known virus or worm attacks in the past few years. With the exception of the "ILoveYou" worm, the release dates of patches that fixed the security vulnerabilities are before the attack dates. It leads people to conclude that patch management is an effective means of risk mitigation; if system administrators are able to apply patches fast enough once vulnerabilities are reported, they will be able to save their systems from attacks.[3]

Table 1

Virus/Worm	Date of Attack	Patch & Release Date	
Melissa	March 26, 1999	MS99-022	January 21, 1999
IloveYou	May 4, 2000	MS00-71	October 5, 2000
Code Red	July 19, 2001	MS01-033	June 18, 2001
Nimda	September 18, 2001	MS01-20	March 29, 2001
Klez	October 25, 2001	MS01-20	March 29, 2001
SQLSlammer	January 25, 2003	MS02-061	October 16, 2002

[1] Schneier, Bruce. Secrets and Lies – Digital Security in a Networked World. New York: John Wiley and Sons, Inc. 2000: 210.
[2] Ulfelder, Steve. "Practical Patch Management", Network World Fusion, October 21, 2002. URL: http://www.nwfusion.com/supp/security2/patch.html
[3] Microsoft Corp. Security Bulletin, TechNet. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp

Applying patches are tedious and complex tasks. Patches have dependencies and prerequisites. Some of them have to be applied in proper sequence otherwise they may not function properly. Some are not compatible with other patches and some patches even require the old patches to be de-installed first before they can be installed. System administrators normally have to go through thorough analysis on all relevant documents on the patches and the systems before they can decide whether the patches are required, the way to apply them properly, and the timing to deploy them.

Patching computing system is also a task that needs to be done perfectly. It only takes one missed or improper patched system to jeopardize the whole computing environment in an organisation.[4]

Augmented to the problem, nowadays most enterprises use several hardware server platforms of different operating systems, and mission critical applications. There has been both an increase of frequency of vulnerabilities discovered and a decrease in the time between a new vulnerability reported and exploited. Thus, system administrators are constantly in a struggle of upgrading their systems with the latest patches and maintaining system stability and availability. Manual methods of applying patches are not quick enough to tackle this time-consuming, tedious and complex task. System administrators are looking for a robust patching solution to solve this long-standing problem.[5]

The purpose of this paper is to discuss some best practices to allow system administrators to gain control of patch management and improve system security. Although this paper is written from the perspective of security patches, a lot of the concepts presented are also valid for non-security related patches.

BEST PRACTICES OF PATCH MANAGEMENT

Patch management is inter-related with other IT security management processes. System administrators rely on information found in the inventory, system configurations and system risk assessment to analyse and decide which system needs to be patched. Applied patches change the system configuration; thus, patch management is a subset of change management. After a patch is applied, patch information has to be updated into the system configuration repository to reflect the current system configuration for new system installations. System administrators who have strong grip of IT system management processes have a head start in patch management.

[4] Ollman, Gunter. "Oh --- That Security Patch". SC Magazine March 2003: 38.
[5] Colville, R., Wagner, R., and Nicolett, M. "Patch Management Benefits, Challenges and Prerequisites", Decision Framework, DF-18-0680, Research Note, Gartner Research, November 4, 2002: 1.

Inventory of Entire IT Infrastructure

There is a saying, "You cannot manage what you don't know." Before system administrators start to tackle patch management, they need to have a good handle of the inventory of computer systems in their entire organisation infrastructure. Due to the high proliferation of computing devices, just taking an account of computing devices that are under the umbrella of the IT department is not sufficient because a lot of equipment nowadays has computing devices embedded in it. Therefore every single piece of equipment that has a computing device embedded in it needs to be accounted for in the inventory. If the organisation is a large global company, the task is even more daunting. For the purpose of patch management, the inventory should at least have the following information:[6]

- The systems that make up the environment
- Operating system (OS), including version
- Function/Classification (Workstation, Internet Web Server, File Server … etc.)
- Applications that are run on the system
- Patch level (service packs, roll-up/cumulative patches, and hotfixes) of the OS and applications
- Any known but unpatched threats to the system and vulnerabilities in them
- An assessment of the impact of the system/device if it is out of service
- Ownership and contact information

Part of the information of inventory can be automated but there is some information still required to be collected manually (e.g. ownership and contact information). Once the inventory is gathered, it should be updated frequently and the information made available to all IT persons who need the information to carry out their duties.

Assess Risk

During the process of applying a patch, the system is often required to be shut down when risk is involved. The system administrators need to meet with the corporate risk executives to understand the risk tolerance of their organisations.[7] They should use the same risk assessment standard of their organisation to rate the risk of systems in their organisation. The system risk rating will be used to evaluate the risk of system outage due to patching. The golden rule, that the risk of

[6] Ulfelder, Steve. "Practical Patch Management", Network World Fusion, October 21, 2002. URL: http://www.nwfusion.com/supp/security2/patch.html
[7] Ibid.

implementing patch should always be less than the risk of not implementing it, should be used by system administrators when they consider whether a certain patch will be deployed.

Adopt Change Management

Applying a patch is a change of system configuration; therefore patch management is a subset of change management. A good change management process has an identified owner, a path for client input, covers the deployment of a change, back out plan, monitors the outcome of change and reviews the audit trail of change process. If there is a strong change management process in the organisation, patch management is just another piece of it. Otherwise it is necessary for the organisation to develop some change control procedures.[8]

Standardise Configurations

According to Gartner, 80% of the enterprises that attempt to deploy patch management automation, without an effort to manage diversity with standardised configurations, will experience a decrease in availability. [9] Based on the information listed in the inventory, computer systems should then be classified into several manageable groups based on their functions, OS, services and protocols that are running. A system configuration standard is then set up for each type of system. The following are some recommendations for system configuration:

- Harden the system's configuration to make the system more secure.[10]
  - Avoid the default installation. Do not install services that are not needed to run on the system.
  - Bundle patches that have been approved, tested and deployed in production with the installation of new systems.
  - Avoid configuring multi-vulnerable services on one single box (e.g. Microsoft IIS Server, Microsoft SQLServer, FTP Server, Mail Server, DNS Server and file server). This will allow you to apply patches only on systems that are subjected to newly reported vulnerabilities and cut down overall number of patches required. This gives you the ability to set up filters on routing and switching devices and create different security zones based on services and protocols that systems run.

---

[8] Microsoft Corp. "Security Operations Guide for Windows 2000 Server" Chapter 5 – Patch Management, TechNet. September 2002: 3. URL: http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/secops05.asp

[9] Colville, R., Wagner, R., and Nicolett, M. "Patch Management Benefits, Challenges and Prerequisites", Decision Framework, DF-18-0680, Research Note, Gartner Research, November 4, 2002: 1.

[10] SANS Institute, The. "SANS Security Essentials II: Network Security", August 2002:32

- Automate installation processes as much as possible to ensure systems are conforming to standards; otherwise set up some quality control processes, such as checklists, and a system certification process to ensure systems are conforming to standards.

- Communicate standards of installation to suppliers of systems that have embedded computing devices.

- Train system administrators on how to configure systems and adhere to the standards of system configurations to set up systems.

- Simplify the computing environment and maintain reasonably generic operating systems and application versions. This does not cut down the security risk but it will cut down the workload necessary to identify patches, test and deploy patches in a more efficient manner.

- Update installation points and configuration repository after patches are successfully applied and ensure new patches are also included in the new system installation.

Standardised system configuration does not imply every system has to conform to a standard of system configuration but rather a majority of them (say 80%) are conformed to standards.

Secure the Supply Chain of Patches

There are some software or OS vendors that only deliver patches to their customers with valid software maintenance agreements. Periodically system administrators should ensure they have valid access to patches and fixes from their system vendors.[11]

Patches represent an entry point to an organisation's infrastructure. There are some patch delivery processes by some system vendors such as Symantec Norton Antivirus "LiveUpdate" and Microsoft SUS which cause concern in the information security community. The vendors allow their customers to directly hook up their systems to receive patches automatically. This delivery mechanism can potentially expose the systems to be attractive targets for attacks and make the customer's environment more vulnerable.[12] Instead of relying on these automatic systems, system administrators should evaluate their environments and secure these systems from attacks.

---

[11] Fisher, Dennis. "Patch as Patch Can", December 9, 2002. URL: http://www.eweek.com/print_article/0,3668,a=34545,00.asp (May 12, 2003).

[12] Colville, R., Wagner, R., and Nicolett, M. "Patch Management Benefits, Challenges and Prerequisites", Decision Framework, DF-18-0680, Research Note, Gartner Research, November 4, 2002.: 3

Nowadays a lot of Internet worms propagated by electronic mail mimic themselves from legitimate software or hardware companies distributing system patches and lure the electronic mail recipients to click on a file attachment to install the patch (e.g. W32.Sobig worm). There are also cases where people have found a virus on brand new cellophane wrapped software distribution diskettes. Therefore, when a patch file is received via distribution diskettes or downloaded via the Internet, the signature of the file must be validated to ensure it is from the right source. Always scan the patch file to ensure it is free of computer viruses or worms before it is installed. Always install a patch file on a test system first.

Study All Relevant Documents

Study all relevant documents of the patch and systems that need to be patched thoroughly and clarify any uncertainty with computer system vendors before a decision to patch is made. This will save a lot of unnecessary effort due to misinterpretation of the patch and system documents.[13]

Test before Deployment of Patches in Production

According to Gartner 80% of the companies who did not test patches before they deployed patches on production systems reported system outages. [14] Patches must be tested before they are applied in production.

Desktop workstations present another challenge. Organisations normally have more desktop computers and these desktop computers have hundreds of applications installed on them. Some larger organisations have over a thousand desktop applications. It is very difficult to test every single application before applying a patch to desktops within a short period of time. Sampling of applications can be selected based on services and protocols they require to run. Use these application samples to test the compatibility of desktop patches. Under critical situations such as a virus outbreak, a patch may have to be applied immediately; a fast track testing methodology must exist. A sampling of desktop systems from the live environment should be identified and ready to use for this purpose.

During the test stage, the tools or scripts that will be used for patch deployment need to be tested. The back out plan or contingent plan needs to be tested as well

[13] Ulfelder, Steve. "Practical Patch Management", Network World Fusion, October 21, 2002. URL: http://www.nwfusion.com/supp/security2/patch.html

[14] Colville, R., Wagner, R., and Nicolett, M. "Patch Management Benefits, Challenges and Prerequisites", Decision Framework, DF-18-0680, Research Note, Gartner Research, November 4, 2002.: 1.

to ensure that, if the patch deployment is not working the way it is supposed to, there is a way to back out of it without causing too much of damage.

Automate Patch Deployment as Much as Possible

Automating patch deployment has two benefits besides saving on labor costs. It deploys patches in a faster manner and it is able to correct security flaws within a relatively short period of time. It also deploys patches in a very controlled manner, allows future trouble-shooting, and manages system problems more straight-forwardly.

Automated patch deployment for standardised computing systems can be easily achieved by automated patch management tools or by some simple scripts.[15] For non-standardised computing systems, they have to be patched manually to minimise system outage.

After testing, when a patch is deployed in production, deploy it to a small percentage of non-critical systems first, say 10% of the system population, and make sure there are sufficient resources to carry out back out processes when necessary. If the deployment is successful, then deploy the patch more aggressively to the rest of the population. Always back up systems and ensure their back ups are in good shape before deployment of a patch in production.[16]

Scan Periodicly for Vulnerabilities

Periodic scanning for vulnerabilities serves two purposes:

- It discovers new or unknown security holes and vulnerabilities in the environment.
- It also acts as quality control for the patch deployment.

There are a lot of vulnerability scanners available. Some automated patch management tools also have vulnerability scanning features as well. It is recommended that if a patch management automation tool is used to deploy patches, a different tool should be used to scan the environment to validate the results of patch deployment. During the patch validation, the system configuration settings before the patch is applied and after the patch is applied should be compared to ensure the configuration settings remain.[17]

---

[15] Microsoft Corp. "Security Operations Guide for Windows 2000 Server" Chapter 5 – Patch Management, TechNet. September 2002. URL: http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/secops05.asp

[16] Ulfelder, Steve. "Practical Patch Management", Network World Fusion, October 21, 2002. URL: http://www.nwfusion.com/supp/security2/patch.html

[17] Ollman, Gunter. "Oh --- That Security Patch". SC Magazine March 2003: 38.

Maintain Good Communication

It is important to have access to the latest news on information security. It will allow you to re-evaluate your position and respond quickly. Subscribe to a well-respected vulnerability database, join various mailing lists of IT security and software vendors, actively surf information security sites and software vendors' Web sites to collect information on vulnerabilities and threats and actively establish industry contacts are ways to improve access to vulnerability news.

All people involved in patch management in the organisation should maintain good communication channels among them. Everybody has to know his/her roles and responsibilities, what to do, and how to do it so that no step of a process is missed. This is particularly important for global organisations that have their networks and computing sites spanning around the globe. A gap analysis between what people think about their roles and responsibilities versus what they are actually required to do during a patching process will ensure everybody knows his/her roles and nothing falls "into the cracks".

A patch tracking system can also help system administrators enhance their communication. It keeps track of which patch has been decided to be applied, who made the decision, the associated risk of the patch, who did the work, any issues along the way when it was tested and, finally, the outcome of the patch deployment in production. It also provides a trail to allow management to evaluate and improve the patch management process.

Use Intrusion Detection System or Intrusion Protection System

There are situations when patches are not applied on systems as quickly as they should because of scheduling problems, other management problems or conflicts between patched applications. An intrusion detection system (IDS) or intrusion protection system (IPS) should be utilised to monitor these unpatched systems.[18] Besides, there are zero-day vulnerabilities. These are vulnerabilities that were not discovered before they were exploited. To have an IDS or IPS monitoring the environment and set off an alarm to alert system administrators is also a mitigation plan. Systems then can be isolated or contained as quickly as possible once intrusion is detected and damage can be minimised.

CONCLUSION

Patch management has been a long-standing IT system management process since the invention of the computer. Today it becomes an information security

[18] Ollman, Gunter. "Oh --- That Security Patch". SC Magazine March 2003: 38.

counter-measures to Internet threats and considered as an important layer of integrating security. Organisations have to be good at patch management to protect themselves in the Internet. To excel in patch management, organisations cannot just strengthen patch management process only; they are required to consider other IT system management processes as well because patch management relies on them to be efficient. Processes such as inventory, system configurations, risk management, change management, system audit, and communication channels should be evaluated and enhanced together with patch management; appropriate security counter-measures should be built in and co-ordinated with all these processes to make patch management a safe, reliable and efficient process to carry out its high profile tasks.

Reference

Andress, Mandy. "Holes in Your Network - Vulnerability-assessment Tools Edge Toward Usefulness in Large Network", Network World Fusion, February 4, 2002. URL: http://www.nwfusion.com/reviews/2002/0204bg.html (4 February 2003).

Colville, R. and Nicolett, M. "Patch Management: Identifying the Vendor Landscape", Markets, M-19-4562, Gartner Research Notes, March 18, 2003.

Colville, R., Wagner, R., and Nicolett, M. "Patch Management Benefits, Challenges and Prerequisites", Decision Framework, DF-18-0680, Research Note, Gartner Research, November 4, 2002.

Fisher, Dennis. "Patch as Patch Can", December 9, 2002. URL: http://www.eweek.com/print_article/0,3668,a=34545,00.asp (May 12, 2003).

Kilpatrick, Ian. "Security Patches and Negative ROI Equal Corporate Stupidity", SC Infosec, April 16, 2003. URL: http://www.infosecnews.com/opinion/2003/04/16_01.htm

Microsoft Corp. "Overview of Security through Deployment", Technet, September 2002. URL: http://www.microsoft.com/technet/security/tips/overview.asp (September 2002)

Microsoft Corp. "Patch Management Service Offerings", Microsoft Solutions, Solution, December 10, 2002.URL: http://www.microsoft.com/solutions/msm/evaluation/overview/patchmgmt.asp

Microsoft Corp. "Security Bulletin", TechNet. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp

Microsoft Corp. "Security Operations Guide for Windows 2000 Server" Chapter 5 – Patch Management, TechNet. September 2002. URL: http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/secops05.asp

Nicolett, M. and Colville, R. "Robust Patch Management Requires Specific Capabilities", Technology, T-19-4570, Gartner Research Note, March 18, 2003

Ollman, Gunter. "Oh --- That Security Patch". SC Magazine March 2003: 38.

SANS Institute, The. "SANS Security Essentials II: Network Security" (August 2002)

Schneier, Bruce. Secrets and Lies – Digital Security in a Networked World. New York: John Wiley and Sons, Inc. 2000.

Sun Microsystems. "Solaris Patch Management: Recommended Strategies", (October 2002)

Tippett, Peter S. "A Patch for IT Security Strategy", Digital Mass, March 18, 2003 URL: http://digitalmass.boston.com/news/globe_story.html?uri=/dailyglobe2/068/business/A_patch_for_IT.shtml

Ulfelder, Steve. "Practical Patch Management", Network World Fusion, October 21, 2002. URL: http://www.nwfusion.com/supp/security2/patch.html

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event