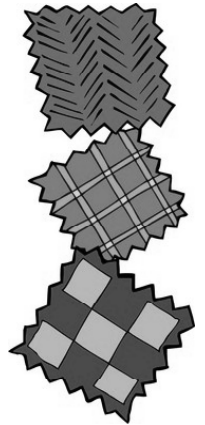


Patches

CSH5 Chapter 40
 “Managing Patches & Vulnerabilities”
 Peter Mell & Karen Kent Scarfone

Topics

- Introduction to Patch & Vulnerability Management
- Why Use Automated Patching Solutions?
- Patch & Vulnerability Management Process
- Patch & Vulnerability Management Issues
- Summary of Major Recommendations



Introduction to Patch & Vulnerability Management

- Vulnerabilities
 - ❑ Flaws
 - ❑ Can be exploited by malicious entities
 - ❑ Obtain unauthorized access / privileges
- Patches
 - ❑ Code to fix flaws / bugs
 - ❑ Can add functionality
 - ❑ Or repair flaws
 - ❑ May lag behind vulnerability disclosures
- Patch & vulnerability management
 - ❑ Systematic processes to prevent exploits



Why Use Automated Patching Solutions? (1)

- Vulnerabilities increasing rapidly [*http://nvd.nist.gov/](http://nvd.nist.gov/)
 - ❑ Jan – Dec 2007: US National Vulnerability Database* – 6691 new vulnerabilities (557/mo, 18/day)
 - ❑ Jan – Dec 2008: 5632
 - ❑ Jan – Dec 2009: 5773
- Damage can be severe: denial of service, data loss, loss of reputation, loss of business....
- Cost of not mitigating damage = WTR
 - ❑ W = workstations
 - ❑ T = time spent fixing problems or lost productivity
 - ❑ R = cost/hour of T

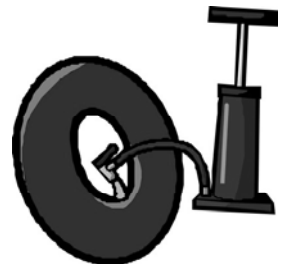
Why Use Automated Patching Solutions (2)

- Manual monitoring for new patches and applying may be labor intensive
 - ❑ E.g., 10 min/day
 - ❑ 10 min/patch per workstation
 - ❑ ... and these costs may add up...
 - ❑ Yet still remain cheaper than disaster
- However, automated patching can be more cost effective
 - ❑ Automatically attend to new patches
 - ❑ Deploy them across entire network
 - ❑ Also more reliable and quicker than manual

Examples of Automated Patch Management Tools

- PatchEasy
- Symantec Altiris Suite
- Desktop Central 7
- Shavlik NetChk Protect

These are examples, not endorsements.



http://www.patcheasy.com/

PATCH EASY™
The easy way to counter cyber threats

HOME | ABOUT PATCH EASY | DOWNLOAD TRIAL | CONTACT | MEDIA

Stop worm related attacks and hacker vulnerabilities

Deploy mission critical patches and protect your network infrastructure. Protect your enterprise from security threats with PatchEasy's automated solutions.

PatchEasy Ver 7.0 coming soon!

Check out PatchEasy Version 7.0 Release Document >>>

FEATURES: PATCH EASY 6.3

- Named Master Agents
- Rollback (Uninstall Patches)
- Reboot Notification
- Scan by IP Range or Subnet
- Sun Solaris and Red Hat Linux Support
- Multi-Locale Support
- Database Size Reduction

Click here for patcheasy 6.3 features

PATCH EASY
Automated patch management from
SECURESYNERGY
The Information Assurance Company
ISO27001 CERTIFIED COMPANY

SecureSynergy is a ISO27001 certified company

FREE Download Trial Ver 6.3

Software Trial (via download - 35MB)
Demo PatchEasy free for 15 days on 5 machines.

Register

Factsheets

What is Patch Management?

... About
... A Way of Life
... Solution Components
... ROI

7

http://www.symantec.com/business/client-management-suite

symantec. Confidence in a connected world.

United States

Home | Business | Partners | Store | About Symantec

Products | Services | Training | Support | Security | Enterprise | Resources | Community

Symantec.com > Business > Products > Business | Client Management Suite

Altiris Client Management Suite

Altiris Client Management Suite tightly integrates industry-leading technologies to reduce the total cost of owning client systems. The suite automates time-consuming and redundant tasks to minimize efforts and costs associated with deploying, managing, securing and troubleshooting client systems so you can gain control of your IT environment.

Release
Purchasing
Data Sheet (PDF)

See	Learn	Buy	Use
<p>Features</p> <ul style="list-style-type: none"> System Requirements New Features White Papers Add-ons Trainers Data Sheets Articles & Interviews Podcasts Press Releases Other Resources 	<p>Key Features</p> <ul style="list-style-type: none"> Comprehensive Client Discovery and Inventory - Optimize software licenses, better support and users, and reduce costs associated with IT deployments and software audits. Industry Leading Imaging & Deployment - Reduce the time associated with imaging and cloning PCs. Reduce support and maintenance costs by deploying standardized, approved, hardware-independent images. Intelligent Software and Patch Management - Update software automatically, safely and remotely. Flexible Remote Assistance - Reduce the open and time associated with troubleshooting and remediating client systems remotely. 	<p>Key Benefits</p> <ul style="list-style-type: none"> Increase visibility with a comprehensive inventory of all hardware and software for each client system. Deploy Windows, Mac, and Linux with a complete touch-free imaging and provisioning. Migrate to the latest version of Windows with less interruption to end-users. Provision applications and software with fewer errors using intelligent, policy-based software deployment. Use vendor provided packages or create approved standard certified-free software packages created with Wile technology. Troubleshoot and fix client PCs with flexible remote management capabilities. Remote control client systems using Symantec patchware technology or use real-time systems management to fix problems without disrupting end-users. Reduce energy and costs associated with client PCs by using intuitive power management policies throughout the organization without losing manageability. 	

http://www.manageengine.com/products/desktop-central/

Store | Reseller | Toll Free US: +1
Australia: +1

Home | Network Management | Server Management | Application Management | Desktop Management | Help Desk / Service Desk | Log Management & Compliance

Products | Downloads | News | Support | Company | Contact Us | Customers | Training | Feedback

Desktop Central 7
Windows Server and Desktop Management Software

Download

Features

- OS Deployment Add-on
- Software Deployment
- Patch Management
- Asset Management
- Remote Control

Supported Networks

- Active Directory
- Work Group
- Novell eDirectory
- WAN
- Roaming Users

More >>

Desktop Central 7 Released
Distribution Points to Optimize Bandwidth Consumption

Free Edition
Manage up to 25 computers

Cut your Energy Bills
by 76% See how?

Windows 7 Compatible

Overview | Features | Demos | Documents | Downloads | Get Quote | Support | Customers | Integration

http://www.shavlik.com/?_k=automated%20patch%20management&_k=c2447d65-e0e2-44cb-8a75-a921

Shavlik Simply Secure.

About Shavlik | Careers | Contact | News

Products | Solutions | Training | Support | Partners | Downloads | Federal | Blogs | Shop

FREE TRIAL DOWNLOAD
BUY NOW
CONTACT US

SHAVLIK AWARDS

TRUSTED BY 70% of the Fortune 500

Windows IT Pro Magazine
names Shavlik NetChk Protect
Editor's Best in Patch Management for 2009.

PROTECT DEFEND CONFIGURE COMPLY TRACK

Security Center

Microsoft Releases 1 Security Bulletin
Security Center Blog

Resources

Why free isn't good enough
Case Studies
Testimonials
Interactive ROI Calculator
3rd Party Technology Audit White Paper
Abaddon Report: Shavlik Integrates Sunbolt Software Technology
PCI Resources
PDCC Resources

Press Releases | In the News | Webinars

10

Patch & Vulnerability Management Process

- Recommended Process
- Creating a System Inventory
- Monitoring for Vulnerabilities, Remediations & Threats
- Prioritizing Vulnerability Remediation
- Creating Organization-Specific Remediation DB
- Testing Remediations
- Deploying Vulnerability Remediations
- Distributing Vulnerability & Remediation Info to Admins
- Verifying Remediation
- Vulnerability Remediation Training

11

Copyright © 2011 M. E. Kabay. All rights reserved.

Recommended Process

- Overview
- Patch & Vulnerability Group (PVG)
- System Administrators (Sysadmins)



12

Copyright © 2011 M. E. Kabay. All rights reserved.

Overview of Process

- Create central, autonomous group for managing patches and vulnerabilities
- May have single PVG or several in hierarchy
- Shift patch administrators from sysadmins to PVG
 - Reduce duplication of effort
 - Save money
 - Reduce errors
- Use standardized configurations for workstations and servers to degree possible
- Keep careful track of inventory and topology

13

Copyright © 2011 M. E. Kabay. All rights reserved.

Patch & Vulnerability Group (PVG)

- Define PVG to include INFOSEC + OPS
 - Sysadmin
 - Intrusion detection
 - Firewall management
 - Operating systems experts
 - Vulnerability scanners
- May be full- or part-time depending on size, complexity of organization & systems
- May rotate staff into group to spread knowledge

14

Copyright © 2011 M. E. Kabay. All rights reserved.

PVG Duties

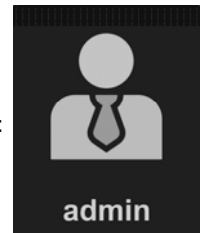
1. Create system inventory
2. Monitor for vulnerabilities, remediations & threats
3. Prioritize vulnerability remediation
4. Create organization-specific remediation database
5. Conduct generic testing of remediations
6. Deploy vulnerabilities remediations
7. Distribute vulnerability & remediation information to local system administrators
8. Perform automated deployment of patches
9. Configure automatic update of applications wherever possible & appropriate
10. Verify vulnerability remediation through NW & host vulnerability scanning
11. Vulnerability remediation training

15

Copyright © 2011 M. E. Kabay. All rights reserved.

System Administrators (Sysadmins)

- Responsible for ensuring that IT resources follow standard configuration defined for organization
- Ensure that resources participate in automated patching system
- Or if using manual patching, coordinate with PVG
- Handle exceptions
 - Trial systems
 - Experimental configurations
 - Prototypes under development



16

Copyright © 2011 M. E. Kabay. All rights reserved.

Creating a System Inventory

- Essential to know exactly what needs protection
- IT Inventory
 - Update constantly / real-time
 - Usually prefer organization-wide DB
 - Suggested fields on p. 40-7
 - Preferably use automated inventory agents
 - Also use bar codes on all components
 - ✓ Systems, peripherals....
 - ✓ Cabling
 - ✓ Network elements (routers, switches...)

17

Copyright © 2011 M. E. Kabay. All rights reserved.

Grouping & Prioritizing IT Resources

- Elements in inventory need *priority levels*
- Reflect degree of criticality
 - Impact of compromise
 - Dependencies – critical patch for recovery
- Can use FIPS PUB 199
 - Standards for Security Categorization of Federal Information and Information Systems*
 - See next slide

18

Copyright © 2011 M. E. Kabay. All rights reserved.

Get to Know the NIST CSRC



http://csrc.nist.gov/publications/PubsFIPS.html

NIST National Institute of Standards and Technology
Information Technology Laboratory

Computer Security Division
Computer Security Resource Center

CSRC HOME GROUPS PUBLICATIONS DRIVERS NEWS & EVENTS ARCHIVE

CATEGORY TYPES

- by Draft Publications
- by FIPS Publications
- by Special Publications
- by NIST IRs
- by ITL Security Bulletins
- Archived FIPS Publications
- Archived Special Publications
- NIST INFORMATION SECURITY DOCUMENT CATEGORIES
- by Topic Clusters
- by Family
- by Legal Requirement

Subscribe to the CSRC Publications Mailing List

CSRC HOME » PUBLICATIONS » BY FIPS PUBLICATIONS

PUBLICATIONS

FIPS Publications

FIPS Publications are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

With the passage of the Federal Information Security Management Act of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards (FIPS). Therefore, the references to the "waiver process" contained in many of the FIPS are no longer applicable. .

FIPS

Number	Date	Title
FIPS 201--1	Mar 2006	Personal Identity Verification (PIV) of Federal Employees and Contractors FIPS-201-1-chng1.pdf

19

NIST CSRC: FIPS 199



FIPS

Number	Date	Title
FIPS 201--1	Mar 2006	Personal Identity Verification (PIV) of Federal Employees and Contractors FIPS-201-1-chng1.pdf
FIPS 200	Mar 2006	Minimum Security Requirements for Federal Information and Information Systems FIPS-200-final-march.pdf
FIPS 199	Feb 2004	Standards for Security Categorization of Federal Information and Information Systems FIPS-PUB-199-final.pdf
FIPS 198--1	Jul 2008	The Keyed-Hash Message Authentication Code (HMAC) FIPS-198-1 final.pdf

Use of IT Inventory & Scope of Related Duties



- Inventory is foundation of PVG operations
 - ❑ Ensure PVG knows which vulnerabilities to look for & to respond to
 - ❑ Checklist for ensuring that all vulnerable systems remediated
- Publication allows sysadmins to spot missing or incorrect components & fix DB
- Managers, security personnel can also use information productively
 - ❑ But restrict access according to permissions as appropriate
 - ❑ E.g., division / department / workgroup

21

Copyright © 2011 M. E. Kabay. All rights reserved.

Monitoring for Vulnerabilities, Remediations & Threats



- Types of Security Concerns
 - ❑ Vulnerabilities
 - ❑ Remediations
 - ❑ Threats (exploits, malware)
- Be on lookout for unauthorized...
 - ❑ Hardware
 - ❑ Software
 - ❑ Configurations



22

Copyright © 2011 M. E. Kabay. All rights reserved.

Tools for Monitoring Vulnerabilities, Remediations & Threats



- Vendor Websites & mailing lists (product-specific newsletters)
- Third-party Web sites (e.g., SANS, CERT-CC®, various alert newsletters)
- Vulnerability scanners
- Vulnerability databases
 - ❑ National Vulnerability Database
- Enterprise patch management tools
- Other notification tools

23

Copyright © 2011 M. E. Kabay. All rights reserved.

http://www.cert.org/

CERT

Software Assurance | Secure Systems | Organizational Security | Coordinated Response | Training

Information for: System Administrators, Developers, Researchers, Managers, Prospective Employees

Welcome to CERT

about us

CERT, the home of the well-known CERT Coordination Center, is located at Carnegie Mellon University's Software Engineering Institute. We study internet security vulnerabilities, research long-term changes in networked systems, and develop information and training to help you improve security.

Our areas of focus

- software assurance
- secure systems
- organizational security
- coordinated response
- training

Time to turn

CERT Spotlight: Podcast Series

What do the experts think?

Business leaders often struggle with the challenge of staying current on relevant topics when they have limited time to devote to the effort. Are you looking for a flexible, time-efficient way to get perspectives and insights directly from security professionals?

Our podcast series features conversations with experts in areas such as security threats, risk management, privacy, and trends. You can choose to listen to the full conversation or select individual sections. Show notes and transcripts are also available.

Announcements

January 20, 2010
New CERT PGP Public Key
CERT has updated its PGP public key. We strongly urge you to encrypt sensitive information.

January 12, 2010
New Podcast Released
The SGMM provides a roadmap to guide an organization's transformation to the smart grid.

December 22, 2009
New Podcast Released
Addressing privacy during software development is just as important as addressing security.

more announcements

headlines

Software Engineering Institute | Carnegie Mellon

Home | About | Contact | FAQ | Jobs | Legal | Site Index
Copyright © 2010 Carnegie Mellon University

24

http://isc.sans.org/

computer security training GIAC My ISC port/ip lookup/search: [input]

Today's Internet Threat Level: GREEN
Handler on Duty: Joel Esler

Handler's Diary: Cisco Security Advisory: Multiple Vulnerabilities in Cisco Unified ...

ISC and Handler Twitter accounts

Today's Diary

previous

If you have more information or corrections regarding our diary, click here to contact us.

Cisco Security Advisory: Multiple Vulnerabilities in Cisco Unified MeetingPlace

Published: 2010-01-28, Last Updated: 2010-01-28 01:28:08 UTC by Joel Esler (Version: 1)

0 comment(s)

Just wanted to call attention these patches released today: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1490b.shtml

Daily Podcast
Listen to our daily summary of security in 5 minutes a day keeps the virus away!

daily ISC Stormcast

Featured Event

SANS 2010 March 6-15 2010
Orlando, FL
Our most comprehensive information security training event of the year... more than 30 courses...

Latest Reading Room Papers

http://www.theregister.co.uk/

Log in | Sign up

The Register
Bringing the hand that feeds IT

Hardware Software Music & Media Networks Security Public sector Business Science Odds & Sods

Exchange Online SharePoint Online Try out Microsoft's cloud services with this free demo.

Ubuntu Firefox shuns Google for Yahoo! search
Microsoft to hand Linux development

Server: 23 Jan 01:18 Oracle to invest in Sparc Iron, clusters
No oracles and twosies

IT Director: 23 Jan 01:18 NewScale spruces IT storefrontware
IT's internal Amazon

Application: 27 Jan 21:10 Ellison to recruit thousands for Sun integration army
Linux needs to grow up

Media and Music: 27 Jan 21:01 Apple's iPad - tat iPhone without the phone
Don't check loans: online IT show

Weekly: 27 Jan 21:03 IE Windows vuln coughs up local files
Print listings, higher scale change

Comment: The tablet that can't multitask

South African Business Journal Awards Verified by Visa Sun shops

If you have questions about upgrading your memory, Crucial has the answers.

crucial The Memory Expert

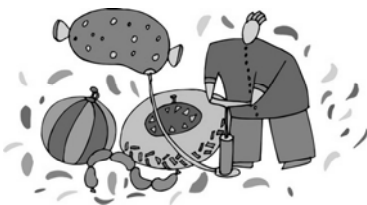
TID #200 TECH TIPS

TOP STORIES MOST READ MOST COMMENTED

Prioritizing Vulnerability Remediation



- Determine significance of threat or vulnerability
- Determine existence, extent & spread of related malware & exploits
- Determine risks involved in applying patch or nonpatch remediation
 - Use external sources of information
 - PVG is not a research group



27

Copyright © 2011 M. E. Kabay. All rights reserved.

Creating Organization-Specific Remediation DB



- Enterprise patch-management tools establish DB for known inventory in organization
- May have to maintain own small DB or manual list of exceptions
- Include threat assessment information
 - Useful in business-continuity (BC) & disaster recovery planning (DRP)
- Include copy of every patch used or planned
 - Can avoid problems of rush on Website

28

Copyright © 2011 M. E. Kabay. All rights reserved.

Testing Remediations



- Standardized configurations allow easy testing of patches on isolated systems
 - Keep standard for test & development only
 - Avoid danger of installing bad patch on production systems
- Eliminate need for redundant, costly testing on all local systems
- But critically important to maintain validity of system *image* so that patches really going to standard configs!
- See extensive list of precautions for testing on pp 40.12 – 40.13 of text

29

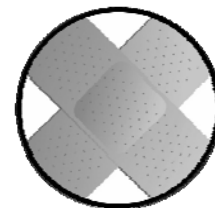
Copyright © 2011 M. E. Kabay. All rights reserved.

Deploying Vulnerability Remediations



3 primary methods of remediation

- Applying security patch ("fix" or "hotfix")
 - Modifies defective code
 - Be sure to download only from safe sites – vendor site usually safe
- Configuration adjustment
 - Change parameter(s); e.g.,
 - ✓ Disabling services
 - ✓ Changing firewall settings
 - ✓ Altering router settings
 - ✓ Modifying registry settings
- Software removal
 - Generally advised to run only essential processes / services on production systems



30

Copyright © 2011 M. E. Kabay. All rights reserved.

Delaying Patch Installations

- Some patches have been discovered to be defective
 - ❑ Caused more problems than they solved
 - ❑ Therefore some admins are gun-shy: delay installation of patches by reflex
- PVG should document, analyze & discuss deviations from recommended installations
 - ❑ Threat level
 - ❑ Risk of compromise
 - ❑ Consequences of compromise



Copyright © 2011 M. E. Kabay. All rights reserved.

Distributing Vulnerability & Remediation Info to Admins

- Primary mechanism: automated patch management software (PMS)
- Emergencies (e.g., failure of PMS) may require alternative channels
 - ❑ Plan for these backup channels in advance
 - ❑ Maintain security
 - ❑ Establish authenticity of patch instruction
 - ❑ Establish authenticity & integrity of patch itself



Copyright © 2011 M. E. Kabay. All rights reserved.

Verifying Remediation

- Must be sure patches have in fact been installed
 - ❑ Correctly &
 - ❑ On all appropriate targets
- Performing Vulnerability Scanning
 - ❑ Automated systems can locate unpatched vulnerabilities independently
 - ❑ Also map network topology to identify undocumented systems
- Reviewing Patch Logs
 - ❑ Useful in detailed forensic-level analysis
 - ❑ Help identify installation problems, aborts
- Checking Patch Levels
 - ❑ NAC* can check for patch levels (e.g., CISCO Clean Access Agent)



*Network Access Agent

Copyright © 2011 M. E. Kabay. All rights reserved.

Vulnerability Remediation Training

- Corporate policy may allow software other than what the PVG controls to be used
 - ❑ Thus PVG will have to train local sysadmins in patching process
 - ❑ Must identify which software requires manual monitoring for patches
- Centralized patch distribution may not apply to all systems
 - ❑ Then users may be involved in collaboration to update systems
 - ❑ Critically important to convince users & sysadmins of value of cooperation

Copyright © 2011 M. E. Kabay. All rights reserved.

Patch & Vulnerability Management Issues

- Enterprise Patching Solutions
 - ❑ Types of Patching Solutions
 - ✓ Nonagent Patching Solutions
 - ✓ Agent-Based Patching Solutions
 - ✓ Advantages & Disadvantages
 - ❑ Integrated SW Inventory Capabilities
 - ❑ Integrated Vulnerability Scanning Capabilities
 - ❑ Deployment Strategies
- Reducing Need to Patch by Smart Purchasing
- Using Standardized Configurations
- Patching After Security Compromise

§40.4 is beyond the level expected for an undergraduate IA mgmt course.

Copyright © 2011 M. E. Kabay. All rights reserved.

Summary of Major Recommendations (1)

1. Create patch & vulnerability group
2. Continuously monitor for vulnerabilities, remediations & threats
3. Prioritize patch application & use phased deployments as appropriate
4. Test patches prior to deployment
5. Deploy enterprise-wide automated patching solutions
6. Use automatically updating applications as appropriate
7. Create inventory of all IT assets

Copyright © 2011 M. E. Kabay. All rights reserved.

Summary of Major Recommendations (2)



8. Use standardized configurations for IT resources as much as possible
9. Verify that vulnerabilities have been remediated.
10. Consistently measure effectiveness of organization's patch & vulnerability management program and apply corrective actions as necessary
11. Train applicable staff on vulnerability monitoring and remediation techniques
12. Periodically test effectiveness of organization's patch and vulnerability management program.



DISCUSSION