# Idaho Technology Authority (ITA)

# ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

### Category: G570 – PATCHING & VULNERABILITY MANAGEMENT

**CONTENTS:**



## I. DEFINITION

Agency – All State departments, boards, commissions, councils and institutions of higher education; but not elected constitutional officers and their staffs, the legislature and its staff, or the judiciary (per Idaho Code, 67-5745 [A]).

Application – Any data entry, update, query, or report program that processes data for a user.

Patch – Additional piece of software code developed to address problems or vulnerabilities (commonly called “bugs”) in software.

Remediation – The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are: installing a patch, adjusting configuration settings, or uninstalling a software application.

Risk – The probability that a particular threat will exploit a particular vulnerability.

Risk Management – The process of identifying, assessing, and reducing risk to an acceptable level and implementing the right mechanisms to maintain that level of risk.

System – A computer, server, or IT device (e.g. router, switch, gateway, firewall) to include the hardware, operating system software, and installed applications.

Threat – Any circumstance or event, deliberate or unintentional, with the potential for causing harm to a system.

Vulnerability – A flaw in the design or configuration of software that has security implications. A vulnerability can be exploited by a malicious entity to gain greater access or privileges than is authorized.

## II. RATIONALE

This guideline provides recommendations to state government organizations on how to implement a patching and vulnerability management process. The concepts contained within this guideline are intended to assist an agency in developing a new vulnerability management process or to enhance its existing process.

## III. GUIDELINE

As outlined within ITA Policy P4520, *Patching and Vulnerability Management*, each agency must have an established process to mitigate IT vulnerabilities. At a minimum, the policy requires five steps to ensure the agency systematically addresses vulnerability management. This guideline provides ideas on how to implement those steps.

Each agency should consider these suggestions to be the minimum recommendations for a vulnerability management process.

1. Create and maintain an inventory of the agency's IT systems.

    A. The agency should identify all IT systems requiring protection by using their existing inventory or by developing a new inventory. This inventory should be reviewed and validated to ensure all IT systems (to include operating systems and software) are identified and accurately annotated.

    B. Once an IT inventory has been validated, the agency should establish a priority listing for the systems identified on the inventory. This priority listing should clearly identify the agency's IT systems from most critical to least critical. The agency's business management should be involved in determining the criticality of a system to the organization. This resulting list enables the agency to group systems, based on business criticality, in order to quickly identify and address the risks associated with vulnerabilities that could impact the agency's most critical operations.

    C. Many organizations manually document their IT inventories; however, due to the rapid change of technology and software, such data is often inaccurate since it is updated infrequently. The agency should consider using commercially available automated inventory management tools whenever possible. These tools can actively monitor changes in the IT environment and consolidate this information in a central database for accurate and quick reference.

2. Monitor security resources for vulnerabilities and remediations.

    A. The agency should ensure one or more personnel (e.g. primary/alternate Agency IT Security Coordinators) are regularly monitoring security resources

for vulnerability announcements, patch/non-patch remediations, and threats that correspond to the systems, operating systems, and software within the agency's IT inventory. New vulnerabilities are announced daily; therefore, it is essential that these personnel are actively monitoring the appropriate resources for relevant vulnerability information.

B. At a minimum, the following resources and tools are recommended for identifying new vulnerabilities and remediations:

   i. Subscribe to vendor security mailing lists and periodically monitor vendor web sites for security announcements/patches.

   ii. Subscribe to third-party mailing lists that highlight the most critical vulnerabilities (e.g. US-CERT Cyber Security Alerts).

   iii. Implement an automated patch management tool to obtain all available remediations for the agency's software. An automated patch management tool can actively monitor vendor web sites for any recently announced remediations and subsequently retrieve the most recent patches from the specified vendors.

C. The agency shall review and implement corrective actions described in the Multi-State Information Sharing and Analysis Center (MS-ISAC) security bulletins. These bulletins are sent in a timely manner to the primary and alternate Agency IT Security Coordinator from the Statewide Cyber Security Coordinator. Reference ITA Policy P4520 (*Patching and Vulnerability Management*) for reporting compliance with these security bulletins.

D. The agency should consider subscribing to commercially provided security alert and intelligence services. These services typically provide customized vulnerability and malicious code alerts to inform an organization of the most recent security threats. Along with relevant alerts, these services provide actionable guidance on how to mitigate the risks associated with new threats.

E. A list of recommended patch and vulnerability resources is provided in Appendix A.

3. Prioritize vulnerability remediation based upon threat and potential impact.

   A. When setting priorities for vulnerability remediation, the agency should consider each threat and its potential impact on the organization. When assessing these priorities, the agency should:

      i. Determine the significance of the threat or vulnerability.

1. Establish which systems are vulnerable and/or exposed. The primary focus should initially be on those systems that are most essential for business operations (reference the system criticality prioritization completed earlier in step 1).

2. Evaluate the impact on the agency's operations, network and systems, if the vulnerability was to be exploited.

ii. Determine the existence, extent, and spread of related worms, viruses, or exploits associated with this vulnerability. Determine whether malicious code has been published and/or distributed. If malicious code already exists, the agency should consider the extent of potential damage caused by such code.

iii. Determine the risks involved with applying the patch/non-patch remediation.

4. Mitigate vulnerabilities in a timely manner.

A. Before applying a patch (or taking other non-patch remediation), the agency should test the remediation on non-production systems prior to deploying it on production systems.

i. If non-production systems are not available for testing purposes, the agency should apply the patch (or non-patch remediation) at a time of least use, while also ensuring sufficient time to recover from any unforeseen problems.

B. In addition to testing the remediation, the following precautions should be followed:

i. Check the vendor-provided patch against any authenticity methods provided (e.g. cryptographic checksum, Pretty Good Privacy (PGP) signature, etc).

ii. Run a virus scan on all patches before installation.

iii. Identify the experiences other organizations (e.g. state government entities, corporations) have had installing a new patch or applying other remediation action. Through these experiences, the agency can identify any potential issues that could impact the agency's operations.

iv. Consider the ability to "undo" or uninstall a patch. If a patch does not provide this capability, the agency should consider the need for more thorough testing prior to deployment.

C. Before applying a patch or non-patch remediation, the agency should conduct a full backup of the system(s).

D. Vulnerability remediation should be deployed in accordance with the prioritization determined in step 3. However, the remediation should be applied to all systems that have the vulnerability, even for systems that are not at immediate risk of exploitation.

E. The vulnerability remediation should be incorporated into the agency's standard system builds and configurations.

F. The agency should consider the use of automated patch management tools to reduce the burden of deploying patches to multiple systems. Widespread manual patching is ineffective since the number of patches needed to be installed continues to grow, coupled with the fact that attackers continue to develop exploit code more rapidly.

G. A list of common automated patch management tools is provided in Appendix B.

5. Confirm that remediation actions have been applied.

   A. The agency should verify that the remediation of the vulnerability has been accomplished as intended. Such verification can be accomplished in many ways, to include:

      i. Verify the files or configuration settings have been changed in accordance with the vendor's documentation.

      ii. Scan the host with a vulnerability scanner that is capable of detecting known vulnerabilities.

         1. Only trained, experienced personnel should use a vulnerability scanner within the agency.

         2. Vulnerability scanning should be coordinated with the agency's IT management prior to execution.

   B. Verify whether the recommended patch was installed by reviewing patch logs.

   C. Employ exploit procedures or code and attempt to exploit the vulnerability (i.e. penetration testing).

      i. Only trained, experienced personnel should perform exploit tests, since this often involves launching an actual attack.

ii. This type of testing should be used only when necessary and should always be coordinated with the agency's IT management prior to execution.

6. The agency should use standardized configurations for their IT systems to reduce the labor involved in identifying, testing, and applying patches. By using standard configurations, the agency will achieve a higher level of consistency in deploying patches, which will lead to improved security.

   A. Standard configurations should be defined for each major group of IT systems (e.g. routers, workstations, servers). Standardization efforts should focus on the types of IT systems that make up a significant portion of the agency's IT inventory.

   B. A standard configuration may include the following:

      i. Hardware type and model

      ii. Operating system version and patch level

      iii. Major installed applications (version and patch level)

Security settings for the operating system and applications

## IV. PROCEDURE REFERENCE

Policies for mobile devices are detailed in ITA Information Technology Enterprise Policies *P4110 – Agency IT Security Coordinator* and *P4520 – Patch and Vulnerability Management.*

NIST Special Publication 800-40 (version 2.0), *Creating a Patch and Vulnerability Management Program, http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf*

## V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

## REVISION HISTORY

07/01/13 – Changed "ITRMC" to "ITA".

6/16/09 – Added Procedure Reference, Contact Information and Revision History to this guideline; changed the layout and deleted References and Timeline.

Effective Date: May 16, 2006

## G570 – PATCHING & VULNERABILITY MANAGEMENT
## APPENDIX A: RECOMMENDED PATCH AND VULNERABILITY RESOURCES

The following security resources are provided as reference material only. Agencies subject to ITA standards should either use the ITA approved standard/product or apply for an exemption in accordance with ITA Policy P1010 (http://ita.idaho.gov/psg/p1010.pdf). The ITA does recognize that several organizations are not subject to ITA Standards; therefore, this list provides a cross-section of resources for the most common software and technologies used throughout various industries.

### General Vulnerability Management Resources

| Resource Name | Web Site |
|---|---|
| US-CERT National Cyber Alert System | http://www.us-cert.gov/cas/ |
| US-CERT National Vulnerability Database | http://nvd.nist.gov/ |
| US-CERT Vulnerability Notes Database | http://www.kb.cert.org/vuls/ |
| Open Source Vulnerability Database | http://www.osvdb.org/ |
| SecurityFocus Vulnerability Database | http://www.securityfocus.com/vulnerabilities |

### Common Operating Systems

| Vendor | Web Site |
|---|---|
| **Apple** | |
| Apple Support | http://www.apple.com/support/ |
| Apple Downloads | http://www.apple.com/support/downloads/ |
| **Cisco** | |
| Products & Services Security Advisories | http://www.cisco.com/en/US/products/products_security_advisories_listing.html |
| Technical Support & Documentation | http://www.cisco.com/en/US/support/index.html |
| **Microsoft** | |
| Microsoft Download Center | http://www.microsoft.com/downloads/search.aspx?displaylang=en |
| Microsoft Help and Support | http://support.microsoft.com/default.aspx |
| Microsoft Security Home Page | http://www.microsoft.com/security/default.mspx |
| Microsoft Security Notification Service | http://www.microsoft.com/technet/security/bulletin/notify.mspx |

| | |
|---|---|
| Microsoft Windows Update | http://windowsupdate.microsoft.com/ |
| Security Bulletins | http://www.microsoft.com/security/bulletins/alerts.mspx |
| **Novell** | |
| Novell Security | http://www.novell.com/products/security.html |
| Novell Support | http://support.novell.com/ |
| **Sun** | |
| Solaris Download | http://www.sun.com/software/solaris/get.jsp |
| Solaris Live Upgrade | http://www.sun.com/software/solaris/liveupgrade/ |
| Sun Update Connection--Patches and Updates | http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage |
| SunSolve Online | http://sunsolve.sun.com/ |

## Common Client Applications

| Product Line | Vendor | Web Site |
|---|---|---|
| **Compression Utilities** | | |
| PKZip | PKWare | http://www.pkware.com/business_and_developers/support/updates/ |
| WinZip | WinZip Computing | http://www.winzip.com/downwzeval.htm |
| **E-mail Clients** | | |
| Groupwise | Novell | http://www.novell.com/support/products/groupwise/ |
| Lotus Notes | IBM | http://www-306.ibm.com/software/lotus/support/notes/support.html |
| Outlook | Microsoft | http://office.microsoft.com/en-us/officeupdate/default.aspx |
| **Multimedia Utilities** | | |
| Flash | Macromedia | http://www.macromedia.com/downloads/ |
| iTunes | Apple | http://www.apple.com/itunes/download/ |
| QuickTime | Apple | http://www.apple.com/support/ |
| Real Player | Real | http://service.real.com/realplayer/security/ |
| Shockwave | Macromedia | http://www.macromedia.com/downloads/ |
| Windows Media Player | Microsoft | http://www.microsoft.com/windows/windowsmedia/player/download/download.aspx |
| **Office Productivity Tools** | | |
| Acrobat | Adobe | http://www.adobe.com/support/downloads |
| Microsoft Office | Microsoft | http://office.microsoft.com/en-us/officeupdate/default.aspx?displaylang=EN |

| Product Line | Vendor | Web Site |
|---|---|---|
| **SSH Clients** | | |
| OpenSSH | OpenBSD Project | http://www.openssh.com/ |
| PuTTY | Simon Tatham | http://www.chiark.greenend.download.html |
| **Web Browsers** | | |
| Firefox | Mozilla | http://www.mozilla.org/security/ |
| Internet Explorer | Microsoft | http://www.microsoft.com/windows/ie/downloads/default.mspx |
| Konqueror | KDE | http://www.kde.org/download/ |
| Mozilla Suite | Mozilla | http://www.mozilla.org/security/ |
| Netscape | Netscape Communications | http://channels.netscape.com/ns/browsers/default.jsp |
| Opera | Opera Software | http://www.opera.com/download/ |

## Common Server Applications

| Product Line | Vendor | Web Site |
|---|---|---|
| **Application Servers** | | |
| Apache Tomcat | Apache Foundation | http://jakarta.apache.org/ |
| Flash Communication Server | Macromedia | http://www.macromedia.updaters.html |
| IBM WebSphere Application Server | IBM | http://www.ibm.com/products/ |
| JRun Application Server | Macromedia | http://www.macromedia.updaters.html |
| Oracle Application Server | Oracle | http://www.oracle.com/ |
| Sun Java System Application Server | Sun | http://www.sun.com/download/20Updates&tab=3 |
| **Collaboration Servers** | | |
| GroupWise | Novell | http://support.novell.com/support_options.html |
| Lotus Domino | IBM | http://www-132.ibm.com/content/home/store_IBMPublicUSA/en_US/Upgrades.html |
| Novell Evolution | Novell | http://support.novell.com/support_options.html |

| | | |
|---|---|---|
| SUSE Linux OpenExchange Server | Novell | http://www.novell.com/products/openexchange/download.html |
| Windows SharePoint Services | Microsoft | http://www.microsoft.com/windowsserver2003/technologies/sharepoint/default.mspx |
| **Database Servers** | | |
| DB2 | IBM | https://www-927.ibm.com/search/SupportSearchWeb/SupportSearch?pageCode=SBD&brand=db2 |
| Informix | IBM | http://www-306.ibm.com/software/data/informix/support/ |
| Microsoft SQL Server | Microsoft | http://www.microsoft.com/sql/downloads/default.asp |
| MySQL | MySQL | http://dev.mysql.com/downloads/ |
| Oracle | Oracle | http://www.oracle.com/technology/software/index.html |
| PostgreSQL | PostgreSQL Global Development Group | http://www.postgresql.org/ftp/source/ |
| **DNS Servers** | | |
| BIND | Internet Systems Consortium | http://www.isc.org/index.pl?/sw/bind/ |
| Microsoft DNS | Microsoft | http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/dns/default.mspx |
| **E-mail Servers** | | |
| Lotus Domino | IBM | http://www-132.ibm.com/content/home/store_IBMPublicUSA/en_US/Upgrades.html |
| Microsoft Exchange | Microsoft | http://www.microsoft.com/exchange/downloads/2003/default.mspx |
| Groupwise | Novell | http://www.novell.com/support/products/groupwise/ |
| **Web Servers** | | |
| Apache HTTP Server | Apache Foundation | http://www.apache.org/dist/httpd/ |
| Microsoft Internet Information Services | Microsoft | http://www.microsoft.com/technet/security/prodtech/IIS.mspx |
| Sun Java System Web Server | Sun | http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage |

## Common Enterprise Firewalls

| Product Line | Vendor | Web Site |
|---|---|---|
| Cisco PIX | Cisco Systems | http://www.cisco.com/en/US/support/index.html |
| FireWall-1 | Check Point Software Technologies | http://www.checkpoint.com/downloads/index.jsp |
| FortiGate | Fortinet | http://support.fortinet.com |
| NetScreen | Juniper Networks, Inc | http://www.juniper.net/customers/support/ |
| Sidewinder | Secure Computing Corporation | http://www.securecomputing.com/index.cfm?skey=246 |
| Sun Cobalt | Sun | http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/index&nav=patchpage |

## Common Enterprise Network Intrusion Detection and Prevention Systems

| Product Line | Vendor | Web Site |
|---|---|---|
| Cisco IPS | Cisco Systems | http://www.cisco.com/en/US/support/index.html |
| Dragon | Enterasys Networks, Inc. | https://dragon.enterasys.com/ |
| eTrust Intrusion Detection | Computer Associates | http://www.my-etrust.com/Support/TechSupport.aspx |
| IntruShield | Network Associates | http://www.mcafee.com/us/downloads/default.asp |
| ManHunt | Symantec Corporation | http://www.symantec.com/techsupp/enterprise/select_product_updates_nojs.html |
| Netscreen | Netscreen Technologies | http://www.juniper.net/customers/csc/software/ |
| SecureNet | Intrusion Inc. | https://serviceweb.intrusion.com/ |
| Snort | Snort | |
| Proventia | Internet Security Systems | http://www.iss.net/support/ |
| Sentivist | NFR Security | http://www.nfr.com/solutions/support.php |
| Snort | Sourcefire | http://www.snort.org/dl/ |
| Sourcefire | Sourcefire | http://www.sourcefire.com/services/support.html |
| UnityOne | TippingPoint Technologies | http://www.tippingpoint.com/support.html |

## Common Enterprise Antivirus and Antispyware Software

| Vendor & Product | Web Site |
|---|---|
| Central Command AntiVirus | http://www.centralcommand.com/downloads.html |
| F-Secure Anti-Virus | http://www.f-secure.com/products/radar/ |
| Lavasoft Ad-Aware | http://www.lavasoftusa.com/ |
| Microsoft Windows AntiSpyware (Beta) | http://www.microsoft.com/athome/security/spyware/software/howto/default.mspx |
| McAfee VirusScan | http://www.mcafee.com/us/downloads/default.asp |
| Sophos Anti-Virus | http://www.sophos.com/downloads/ide/ |
| Spybot-Search & Destroy | http://www.safer-networking.org/en/download/index.html |
| Symantec AntiVirus | http://www.symantec.com/downloads/ |
| Trend Micro Anti-Spyware and VirusWall | http://kb.trendmicro.com/solutions/search/default.asp |

## Other Common Security Applications

| Product Line | Vendor | Web Site |
|---|---|---|
| **Anti-Spam Servers** | | |
| GFiMailEssentials | GFI Software | http://support.gfi.com/ |
| Kaspersky Anti-Spam | Kaspersky | http://www.kaspersky.com/productupdates/ |
| McAfee SPAMkiller | Network Associates | http://www.mcafee.com/us/downloads/default.asp |
| MailMarshal | NetIQ | http://www.netiq.com/support/default.asp |
| IronMail | Ciphertrust | http://www.ciphertrust.com/support/index.php |
| **Personal Firewalls and Suites** | | |
| BlackIce | Internet Security Systems | http://blackice.iss.net/update_center/ |
| F-Secure Internet Security 2005 | F-Secure | http://support.f-secure.com/enu/home/ |
| Kaspersky Anti-Hacker | Kaspersky Labs | http://www.kaspersky.com/productupdates |
| McAfee Personal | Networks Associates | http://download.mcafee.com/us/upgradeCenter/?cid=11536 |

| Product Line | Vendor | Web Site |
|---|---|---|
| Firewall Plus | Technology, Inc. | |
| Norton Personal Firewall | Symantec | http://www.symantec.com/downloads/ |
| Panda Platinum Internet Security | Panda Software | http://www.pandasoftware.com/download/ |
| PC-cillin Internet Security | Trend Micro | http://www.trendmicro.com/download/product.asp?productid=32 |
| Sygate Personal Firewall | Sygate | http://smb.sygate.com/download_buy.htm |
| Tiny Firewall | Tiny Software | http://www.tinysoftware.com/home/tiny2?s=5375286922906826215A1&&pg=content05&an=tf6_download&cat=cat_tf6 |
| ZoneAlarm | Zone Labs | http://download.zonelabs.com/bin/free/information/zap/releaseHistory.html |
| **VPN Clients** | | |
| Cisco VPN Client | Cisco | http://www.cisco.com/public/sw-center/ |
| NetScreen-Remote | Juniper | http://www.juniper.net/customers/support/ |
| Nortel VPN Client | Nortel | http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=software&tranProduct=10621 |
| VPN-1 SecuRemote, SecureClient | CheckPoint | http://www.checkpoint.com/downloads/index.html |

## G570 – PATCHING & VULNERABILITY MANAGEMENT
## APPENDIX B: COMMON AUTOMATED PATCH MANAGEMENT TOOLS

| Patch Management Tool | Vendor | Web Site |
|---|---|---|
| Altiris Patch Management Solution | Altiris | http://www.altiris.com/products/patchmanagement/ |
| ANSA | Autonomic Software, Inc. | http://www.autonomic-software.com/patch.html |
| BigFix Patch Manager | BigFix, Inc. | http://www.bigfix.com/products/products_patch.html |
| BindView Patch Management | Bindview Corporation | http://www.bindview.com/Solutions/VulnMgmt/ManagePatches.cfm |
| C5 Enterprise Vulnerability Management Suite | Secure Elements | http://www.secure-elements.com/products/ |
| Ecora Patch Manager | Ecora Software | http://www.ecora.com/ecora/products/patchmanager.asp |
| eTrust Vulnerability Manager | Computer Associates International, Inc. | http://www3.ca.com/Solutions/Product.asp?ID=4707 |
| GFI LANguard Network Security Scanner | GFI Software Ltd. | http://www.gfi.com/lannetscan/ |
| Hercules | Citadel Security Software | http://www.citadel.com/hercules.asp |
| HFNetChkPro | Shavlik Technologies, LLC | http://www.shavlik.com/ |
| HP OpenView Patch Manager using Radia | Hewlett-Packard Development Company | http://www.managementsoftware.hp.com/products/radia_patm/index.html |
| Kaseya Patch Management | Kaseya, Inc. | http://www.kaseya.com/prod1/pl/patch_management.phtml |
| LANDesk Patch Manager | LANDesk Software | http://www.landesk.com/Products/Patch/Index.aspx |
| LiveState Patch Manager | Symantec Corporation | http://sea.symantec.com/content/product.cfm?productid=30 |

| Patch Management Tool | Vendor | Web Site |
|---|---|---|
| ManageSoft Security Patch Management | ManageSoft Corporation Ltd. | http://www.managesoft.com/product/patchmanagement/index.xml |
| Marimba Patch Management | BMC Software, Inc. | http://www.marimba.com/products/solutions/patch-mgmt.html |
| NetIQ Vulnerability Manager | NetIQ Corporation | http://www.netiq.com/products/vsm/default.asp |
| Opsware Server Automation System | Opsware, Inc. | http://www.opsware.com/products/serverautomation/patchmgmt/ |
| PatchLink Update | PatchLink Corporation | http://www.patchlink.com/products_services/patchlink_update.html |
| PolicyMaker Software Update | DesktopStandard Corporation | http://www.desktopstandard.com/PolicyMakerSoftwareUpdate.aspx |
| Prism Patch Manager | New Boundary Technologies | http://www.newboundary.com/products/prismpatch/prismpatch_info.htm |
| SecureCentral PatchQuest | AdventNet, Inc. | http://www.securecentral.com/products/patchquest/ |
| Security Update Manager | ConfigureSoft | http://www.configuresoft.com/SUMMain.aspx |
| Service Pack Manager | Gravity Storm Software | http://www.securitybastion.com/ |
| Sitekeeper (Patchkeeper module) | Executive Software | http://www.execsoft.com/sitekeeper/sitekeeper.asp |
| Software Update Services | Microsoft Corporation | http://www.microsoft.com/windowsserversystem/updateservices/evaluation/previous/default.mspx |
| Systems Management Server | Microsoft Corporation | http://www.microsoft.com/smserver/default.asp |
| SysUpdate | SecurityProfiling Inc. | http://www.securityprofiling.com/eng/products/sysupdate.shtml |
| UpdateEXPERT | St. Bernard Software | http://www.patches-management.stbernard.com/ |
| Windows Server Update Services | Microsoft Corporation | http://www.microsoft.com/windowsserversystem/updateservices/default.mspx |
| ZENworks Patch Management | Novell, Inc | http://www.novell.com/products/zenworks/patchmanagement/index.html |