



Ethical Hacking and Countermeasures

Version 6

Module LXV

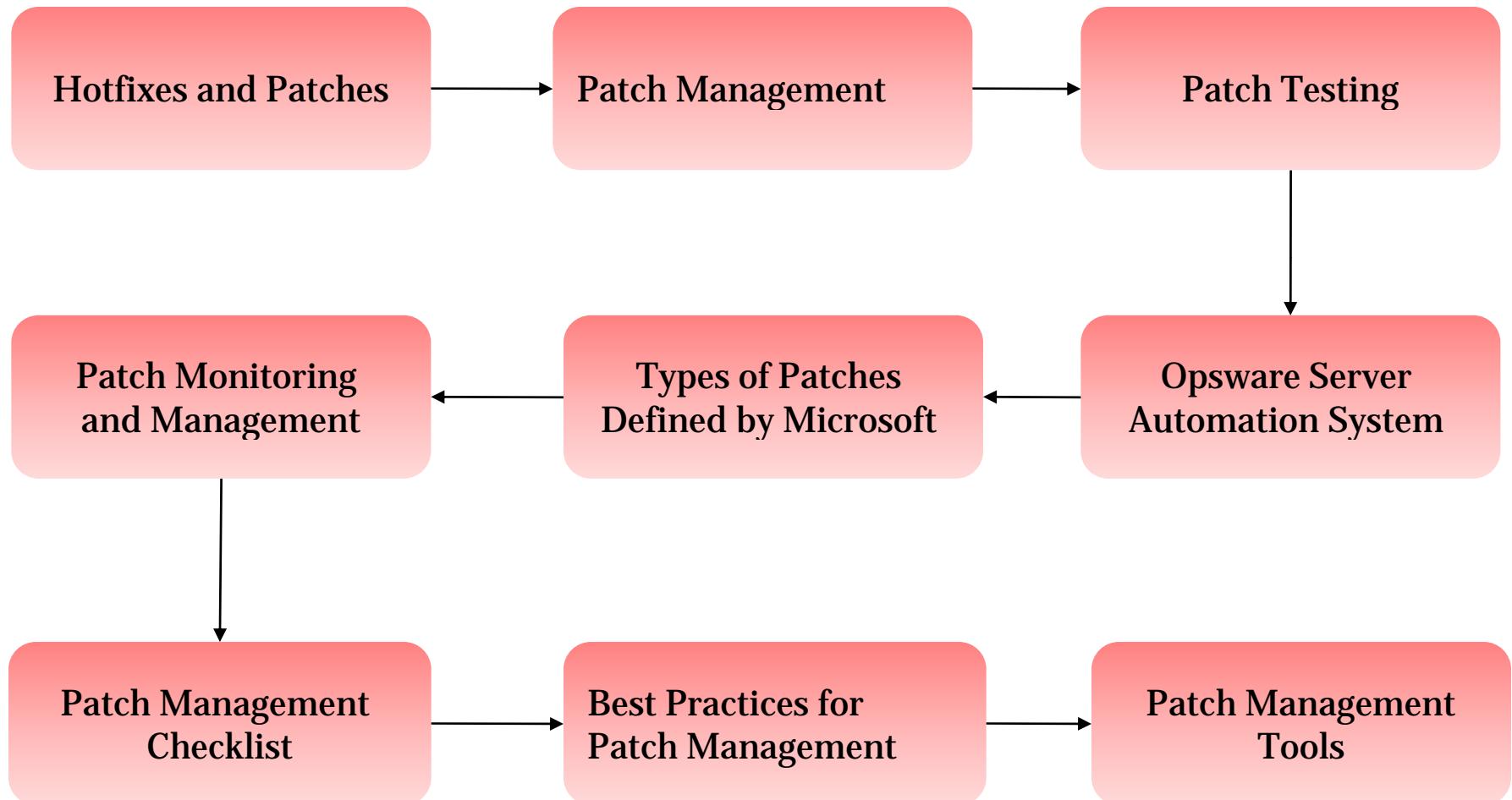
Patch Management



Module Objective

This module will familiarize you with:

- Hotfixes and Patches
- Patch management
- Patch Testing
- Understanding Patch Monitoring and Management
- Types of Patches Defined by Microsoft
- Opsware Server Automation System (SAS)
- Patch Management Checklist
- Best Practices for Patch Management
- Patch Management Tools



Hotfixes and Patches

A hotfix is a code that fixes a bug in a product. The users may be notified through emails or through the vendor's website



Hotfixes are sometimes packaged as a set of fixes known as combined hotfix or service pack



A patch can be considered as a repair job in a piece of programming problem. A patch is the immediate solution provided to users

What is Patch Management

“Patch management is a process to ensure that the appropriate patches are installed on a system”

It involves:

- Choosing, verifying, testing, and applying patches
- Updating previously applied patches with current patches
- Listing patches applied previously to the current software
- Recording repositories, or depots, of patches for easy selection
- Assigning and deploying applied patches



Patch Testing

The first step in patch testing is the verification of patch source and integrity which helps you to ensure that update is valid and it is not altered

The major components of patch testing include:

- Digital signatures
- Checksums
- Integrity verification

Patch testing process takes place in three different categories:

- Testing Patch Installation
- Testing Application Patches
- Testing Service Patches



Understanding Patch Monitoring and Management

Steps in the Patch Management framework are as follows:

1

- Identify the patch location

2

- Identify new patches and verify the patch's authenticity by installing each patch on an isolated system, and determine the time frame

3

- Ensure that both patch testing and risk assessment of patch deployment are processed at one place

4

- Deploy the patch



Understanding Patch Monitoring and Management (cont'd)

Create a Change Process:

- Creating a change management process is like updating software that is required for a system
- Before starting the change management process, switch off the server, and start the process from a small log

Monitor the Patch Process:

- Microsoft suggested a four phase approach that monitors the software updates designed for the management control:
 - Assess
 - Identify
 - Evaluate and Plan
 - Deploy



Types of Patches Defined by Microsoft

Microsoft releases patches to facilitate updates to the Windows OS and Microsoft applications

- Such patches fix known problems, or bugs, in an OS or application and are shipped in three formats:

Hotfixes

- A code that fixes a bug in a product
- Also referred as security fixes or Quick Fix Engineering (QFE) Fixes

Roll-ups

- Merges updates of several Hotfixes into a single update file

Service packs

- An update to a software version that fixes a bug
- Include fixes not previously released and introduces new functionality



TM

Opsware Server Automation System (SAS)

Opsware Server Automation System (SAS) is the data center automation product of choice for heterogeneous IT environments

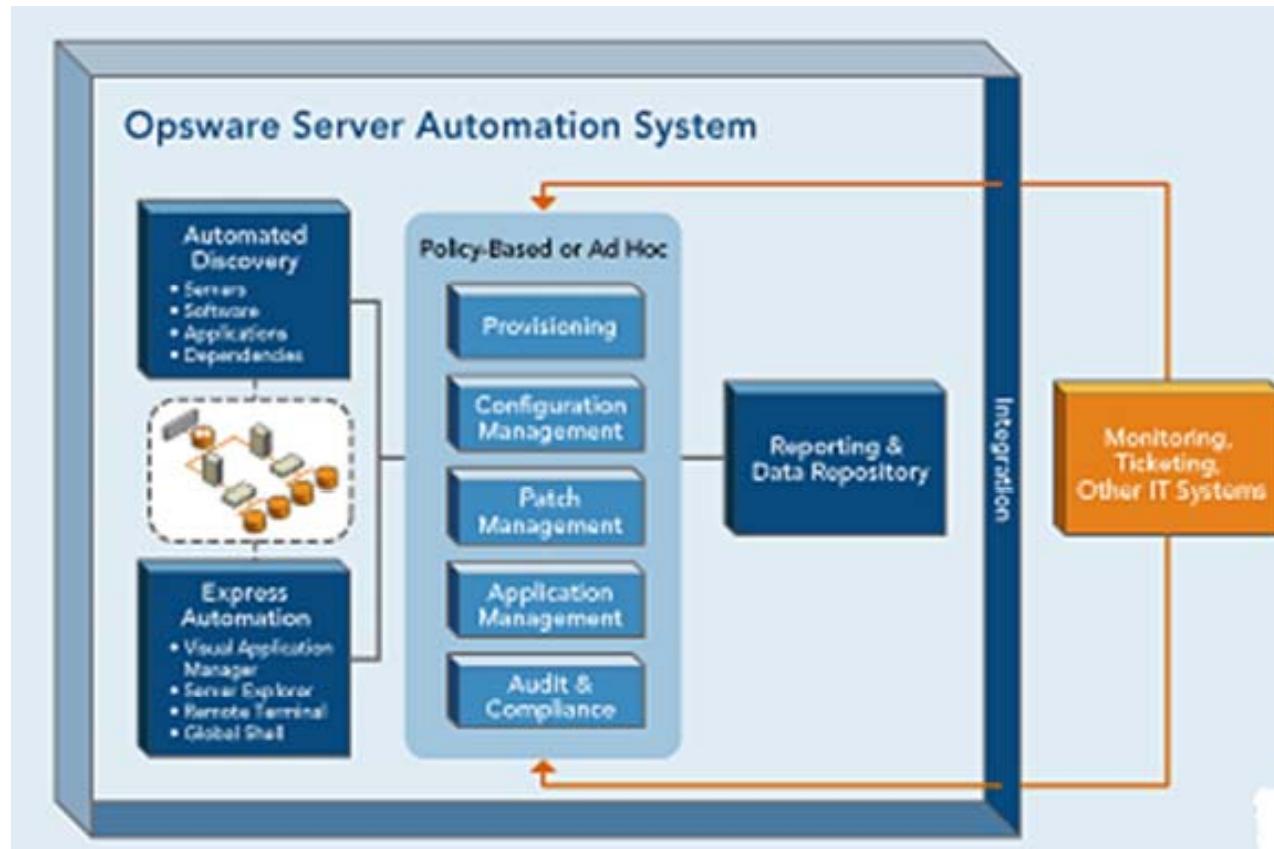
It gives administrators the ability to monitor systems and apply configuration changes across many servers in a uniform fashion

Servers can be provisioned from the same pre-defined baseline from the start

Configuration tracking is used to detect changes that are made and administrators are notified of the changes

The administrator can then use Opsware to rollback the change or propagate the change throughout the server environment

Opsware Server Automation System (SAS) (cont'd)

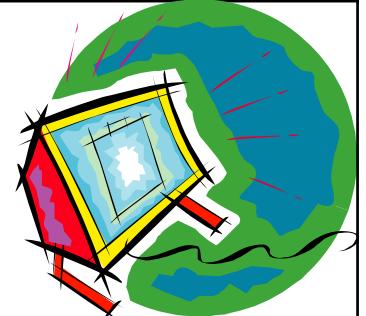




Patch Management Tools

Tool: UpdateExpert

UpdateExpert is a Windows administration program that helps you to secure your systems by remotely managing service packs and hotfixes



Microsoft constantly releases updates for the OS and mission critical applications, which fix security vulnerabilities and system stability problems

UpdateExpert enhances security, keeps systems up-to-date, eliminates sneaker-net, improves system's reliability and QoS



TM

UpdateExpert: Screenshot

The screenshot shows the UpdateExpert application interface. On the left, a tree view displays network resources under "Network: RKAPLAN". A list of machines includes LSEIBERT, LSMITH, MAIL01, MALTAMIRANO, MSEGARS, NETADMIN-LT, PFOWLER, PLEW, RGARCIA, RKAPLAN, RILLSTIG, SBS-DEMO, SLEE, SMAUG-2K, SMEIER, SSWAIN, SSWAIN-LT, TEMP-PC, and TESTER.

The main pane shows a "Research View" table with columns: All, OS, IE, Exchange, SQL Server, IIS, Media. The table lists various Windows patches:

Name	KB Article	Reason for fix	Release Date	Install Date	Language
Q246988i.exe	Q246988	Default Gateway Is Ignored When IRDP Is Enabled	11/24/1999	Not installed	English
Q275713i.exe	Q275713	Access Violation When RAS Is Disabled	10/13/2000	Not installed	English
Q259728i.EXE	Q259728	Windows NT 4.0 Security Patch: IP Fragment Reassembly...	05/08/2000	11/10/2000	English
Q268239i.EXE	Q268239	Windows NT 4 Security Patch: NetBIOS Name Server Prot...	08/18/2000	11/10/2000	English
Q243649i.EXE	Q243649	Windows NT 4.0 Security Patch: Microsoft Print Spooler S...	11/03/1999	11/10/2000	English
Q246954i.exe	Q246954	Unattended RAS Installation Prompts for New IP Address	11/24/1999	Not installed	English
Q262463i.exe	Q262463	Find.exe Returns Extra Lines When Piped	05/09/2000	Not installed	English
Q283001i.exe	Q283001	Windows NT 4.0 Security Patch: Malformed PPTP Packet...	02/14/2001	Not installed	English
Q265714i.EXE	Q265714	Windows NT 4.0 Security Patch: SNMP Parameters Vulnerab...	12/22/2000	Not installed	English
Q280001i.exe	Q280001		02/06/2001	Not installed	English
Q246955i.exe	Q246955		08/25/1999	Not installed	English
Q270001i.exe	Q270001		10/17/2000	Not installed	English
Q262464i.exe	Q262464		06/27/2000	Not installed	English
Q262465i.exe	Q262465		07/17/2000	Not installed	English

A modal dialog box titled "Component Install Wizard" is open, showing the "Install Components" step. It displays the selected machine "RKAPLAN" and the selected hotfix "Q265714i.EXE". The "Installed Time" dropdown is set to "04/27/2001 05:00PM". Under "Options", the "Force apps to close on..." and "Quiet mode" checkboxes are checked. At the bottom are "Done" and "Cancel" buttons.

The background shows a Microsoft Product Support Services window for "Windows NT 4.0 SNMP Parameters Vulnerability". It lists the article ID Q265714, last reviewed on March 27, 2001, and provides a link to "Send to a friend". It also asks if the information helped answer the question.

At the bottom of the screen, there is a status bar with "Ready" and "Live Trial for 150 machines (100 used) exp! Filter".

Page footer: Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Tool: Qfecheck

Qfecheck allows customers to diagnose and eliminate the effects of anomalies in the packaging of hotfixes for Microsoft Windows

Qfecheck.exe determines which hotfixes are installed by reading the information stored in the following registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates



```
G:\CEH\Haja\patch>qfecheck /v
Windows 2000 Hotfix Validation Report for \\SYSTEM5
Report Date: 5/17/2005 2:23pm
Current Service Pack Level: Service Pack 4
Hotfixes Identified:
Q327194: Current on system.
KB820888: Current on system.
KB822831: Current on system.
KB823182: Current on system.
KB823559: Current on system.
KB824105: Current on system.
KB825119: Current on system.
KB826232: Current on system.
KB828035: Current on system.
KB828741: Current on system.
KB828749: Current on system.
KB835732: Current on system.
KB837001: Current on system.
KB839645: Current on system.
KB840315: Current on system.
KB840987: Current on system.
KB841356: Current on system.
KB841533: Current on system.
KB841872: Current on system.
KB841873: Current on system.
KB842526: Current on system.
KB842773: Current on system.
KB871250: Current on system.
KB873333: Current on system.
KB873339: Current on system.
KB885250: Current on system.
KB885835: Current on system.
KB885836: Current on system.
KB888113: Current on system.
KB890047: Current on system.
KB890175: Current on system.
KB890859: Current on system.
KB891711: Current on system.
KB891781: Current on system.
KB893066: Current on system.
KB893086: Current on system.
KB893803: Current on system.
Q818043: Current on system.
```



Tool: HFNetChk

HFNetChk is a command-line tool that enables the administrator to check the patch status of all the machines in a network remotely

It does this function by referring to an XML database that Microsoft constantly updates

```
C:\> C:\WINNT\System32\cmd.exe
MICRON
-----
WINDOWS 2000 SP2
Patch NOT Found MS00-077 Q299796
Patch NOT Found MS00-079 Q276471
Patch NOT Found MS01-007 Q285851
Patch NOT Found MS01-013 Q285156
WARNING MS01-022 Q296441
Patch NOT Found MS01-025 Q296185
Patch NOT Found MS01-037 Q302755
Patch NOT Found MS01-041 Q298012
Internet Information Services 5.0
Patch NOT Found MS01-025 Q296185
Internet Explorer 5.5 SP2
INFORMATION
All necessary hotfixes have been applied
```

cacls.exe Utility

Built-in Windows 2000 utility (cacls.exe) can set access control list (ACLs) permissions globally

To change permissions on all executable files to System:Full, Administrators:Full:

- C:\>cacls.exe c:\myfolder*.exe /T /G System:F
Administrators:F



```
Command Prompt

C:\Snort>cacls.exe *.exe /T /G System:F Administrators:F
Are you sure (Y/N)?y
processed file: C:\Snort\snort.exe

C:\Snort>
```



TM

Tool: Shavlik NetChk Protect

Shavlik NetChk protect is a tool that automates the management of critical security patches, spyware, malware, and unwanted software applications from one console

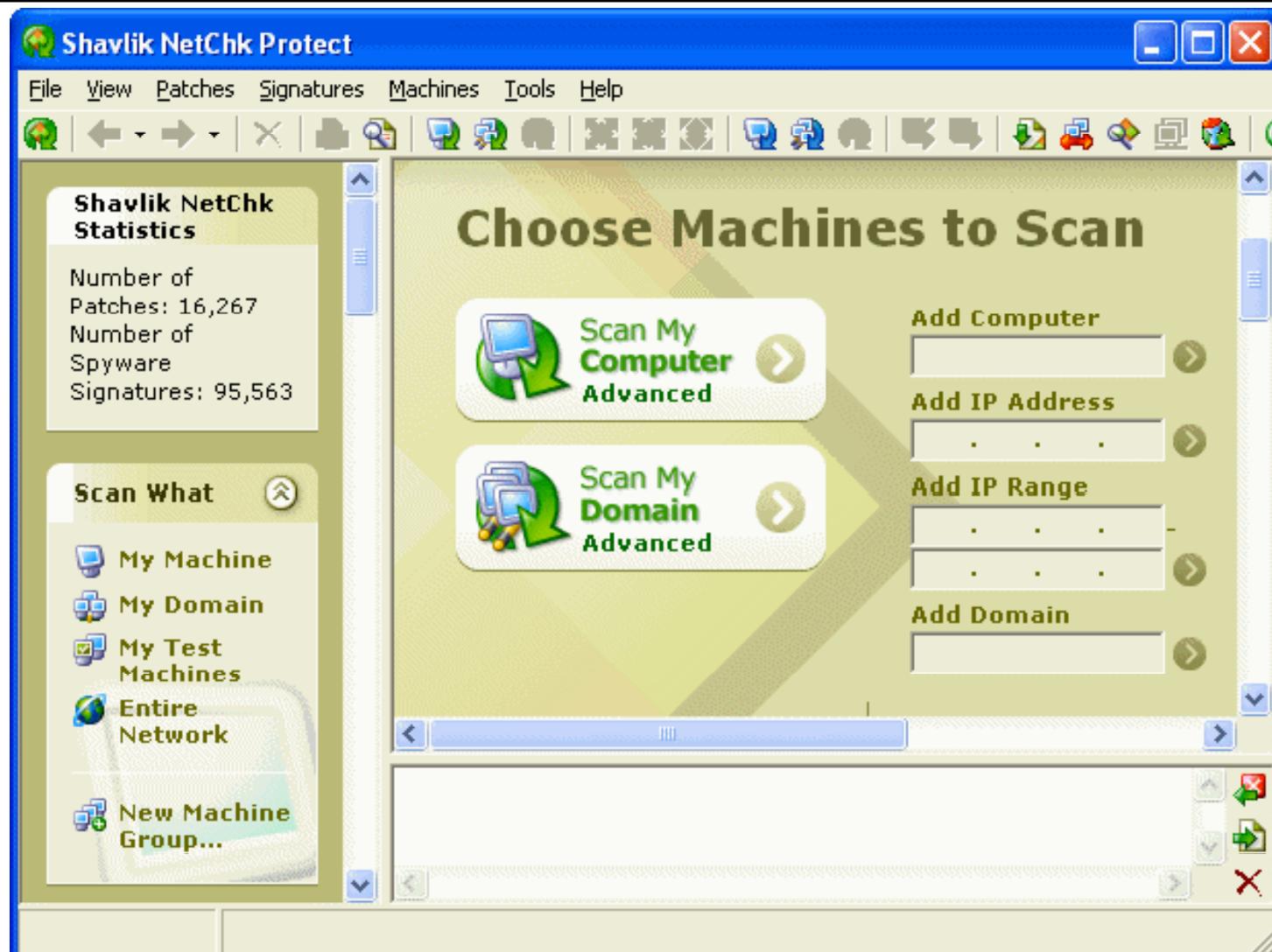
It offers a solution for detecting, removing, and managing critical threats and vulnerabilities with active vulnerability management

Maintain secure, policy-compliant networks through automatic and continuous assessment, remediation, and management

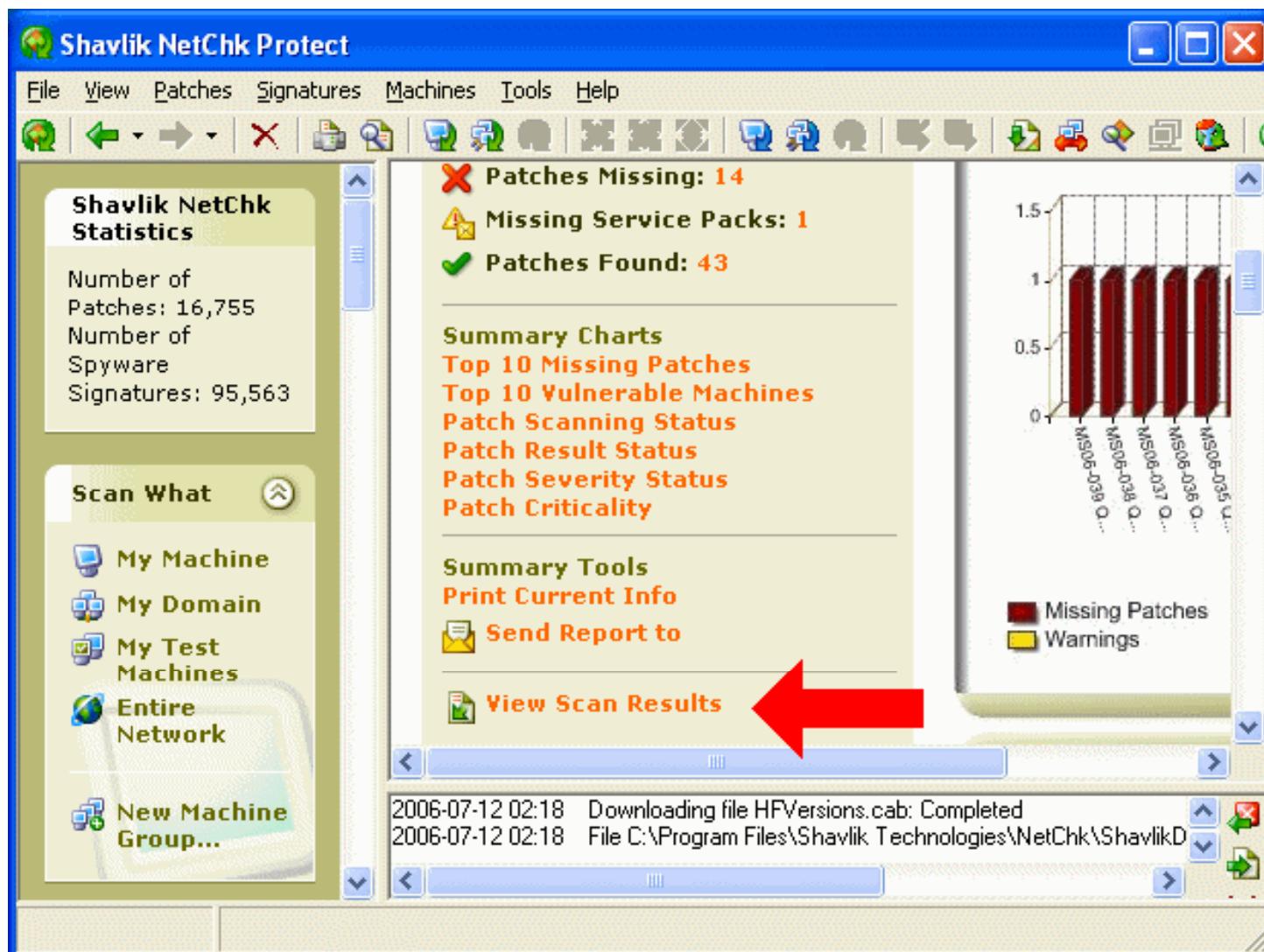
Features:

- Patch Scanning
- Extensive Reporting
- Patch development
- Spyware Management
- Desktop Application Control

Shavlik NetChk Protect: Screenshot 1

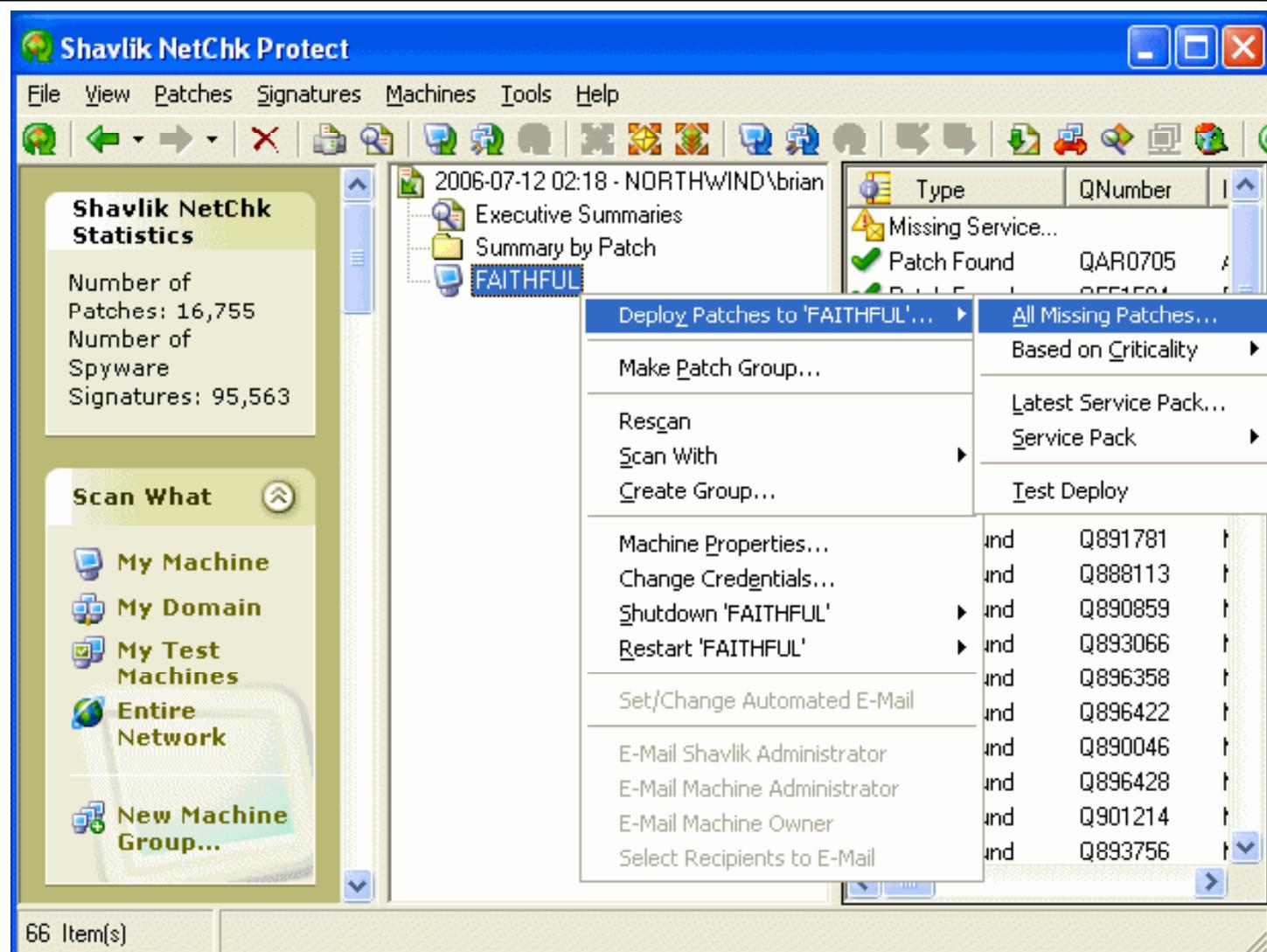


Shavlik NetChk Protect: Screenshot 2





Shavlik NetChk Protect: Screenshot 3





Tool: Kaseya Patch Management

Kaseya Patch Management is used to keep your servers, workstations, and remote computers up-to-date with the latest security patches and updates

It provides the automatic discovery of all missing patches and updates

Features:

- Complete automation for patch discovery and deployment patch
- Location, deployment method, and parameter control reliable and up to date patch data base
- Complete rollback
- Comprehensive history and reporting
- Rapid deployment

Kaseya Patch Management: Screenshot 1

The screenshot shows the Kaseya Patch Management software interface. The top navigation bar includes Home, Audit, Scripts, Monitor, Ticketing, Patch Mgmt (selected), Remote Ctrl, Backup, Reports, Agent, System, and Log Off: Nick. Below the navigation bar are links for Notes, Status, Help, and search/filter options for Machine ID, Rows, Select Machine Group, Select View, and Reset.

The main area displays a configuration dialog titled "Automatically apply all new patches and updates at the scheduled time of day." It includes fields for "Set Auto" (button), "Every day" (dropdown), "at" (dropdown with options 3 am, 4:00, 5:00, Stagger by 5 min.), and "Cancel". There is also a checked checkbox for "Skip if machine offline".

The "Function List" sidebar on the left lists categories: Setup (Scan Machine, Patch Status, Initial Update, Patch History), Schedule Update (Machine Update, Patch Update, Rollback, Automatic Update, Cancel Updates), and Configure (Patch Approval, Reboot Action, File Source, Patch Alert, Windows Auto Update). The "Automatic Update" option under Schedule Update is currently selected.

The main configuration area shows a list of "Machine.Group ID" entries:

- OK KServer
- OK kcheck01.smc.smc
- OK kcheck02.smc.smc

A note indicates that the "Skip if machine offline" option applies to these entries. The "Auto update time" section is also visible.

At the bottom, the footer reads "Powered by  Kaseya - Copyright © 2000-2006 Kaseya. All rights reserved."

Kaseya Patch Management: Screenshot 2

Screenshot of the Kaseya Patch Management interface showing the Patch Mgmt tab selected.

Function List:

- Setup
 - Scan Machine
 - Patch Status** (selected)
 - Initial Update
 - Patch History
- Schedule Update
 - Machine Update
 - Patch Update
 - Rollback
 - Automatic Update
 - Cancel Updates
- Configure
 - Patch Approval
 - Reboot Action
 - File Source
 - Patch Alert
 - Windows Auto Update

Toolbar: Notes, Status, Help, Machine ID, Rows, Select Machine Group, Select View, Reset, << < Select Page > >>, 100, smc.smc, < No View >, Edit...

Message: Verify each machine's configuration successfully downloads and installs patches.

Buttons: Test, Cancel, Auto Refresh Table

WARNING: Test cancels any pending patch in progress. The system resets test results every time [File Source](#) or [Set Credential](#) changes.

Table: Machine Group ID, Installed Patches, Missing Approved, Pending Denied, User Logged In, Failed Patches, Test Results

Machine Group ID	Installed Patches	Missing Approved	Missing Denied	User Logged In	Failed Patches	Test Results
kcheck01.smc.smc	41	52	-	-	-	Passed
kcheck02.smc.smc	41	52	-	-	-	Untested

Powered by  Kaseya - Copyright © 2000-2006 Kaseya. All rights reserved.

Kaseya Patch Management: Screenshot 3

The screenshot shows the Kaseya Patch Management interface. The top navigation bar includes Home, Audit, Scripts, Monitor, Ticketing, Patch Mgmt (selected), Remote Ctrl, Backup, Reports, Agent, System, and Log Off: Nick. Below the navigation bar are buttons for Notes, Status, Help, and links for Machine ID, Rows, Select Machine Group, Select View, Reset, and Edit... The main area has a 'Function List' on the left with categories like Setup, Schedule Update, Configure, and Reboot Action (which is selected). The right side displays a configuration form titled 'Specify how to reboot after applying new patches and updates.' It lists several options for reboot behavior based on user status and time. A table below shows 'Machine.Group ID' and 'Reboot action' for three groups: KServer, kcheck01.smc.smc, and kcheck02.smc.smc. The table indicates that KServer does not reboot but sends an email to bsn@bellcpa.com. The other two groups ask for confirmation if the user does not respond within 5 minutes. At the bottom, it says 'Powered by  Kaseya - Copyright © 2000-2006 Kaseya. All rights reserved.'

Machine.Group ID	Reboot action
KServer	Do not reboot. Send email to bsn@bellcpa.com after update
kcheck01.smc.smc	Ask - Reboot if user does not respond in 5 minutes
kcheck02.smc.smc	Ask - Reboot if user does not respond in 5 minutes



TM

Tool: IBM Tivoli Configuration Manager

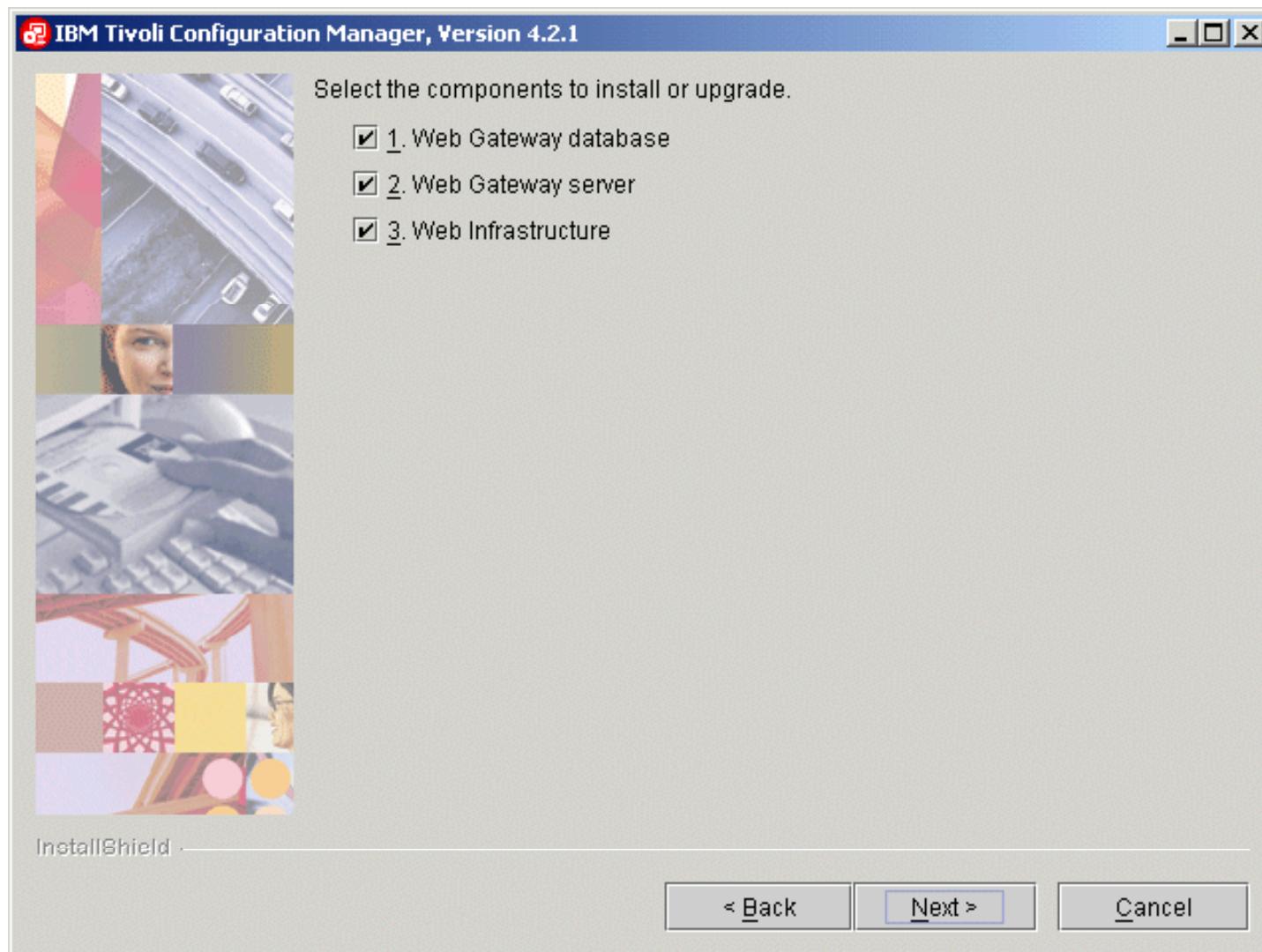
IBM's configuration manager provides Microsoft client and server software patch automation capabilities in distributed environments

Obtains, packages, distributes, and installs Microsoft software patches needed by client systems in distributed customer environments

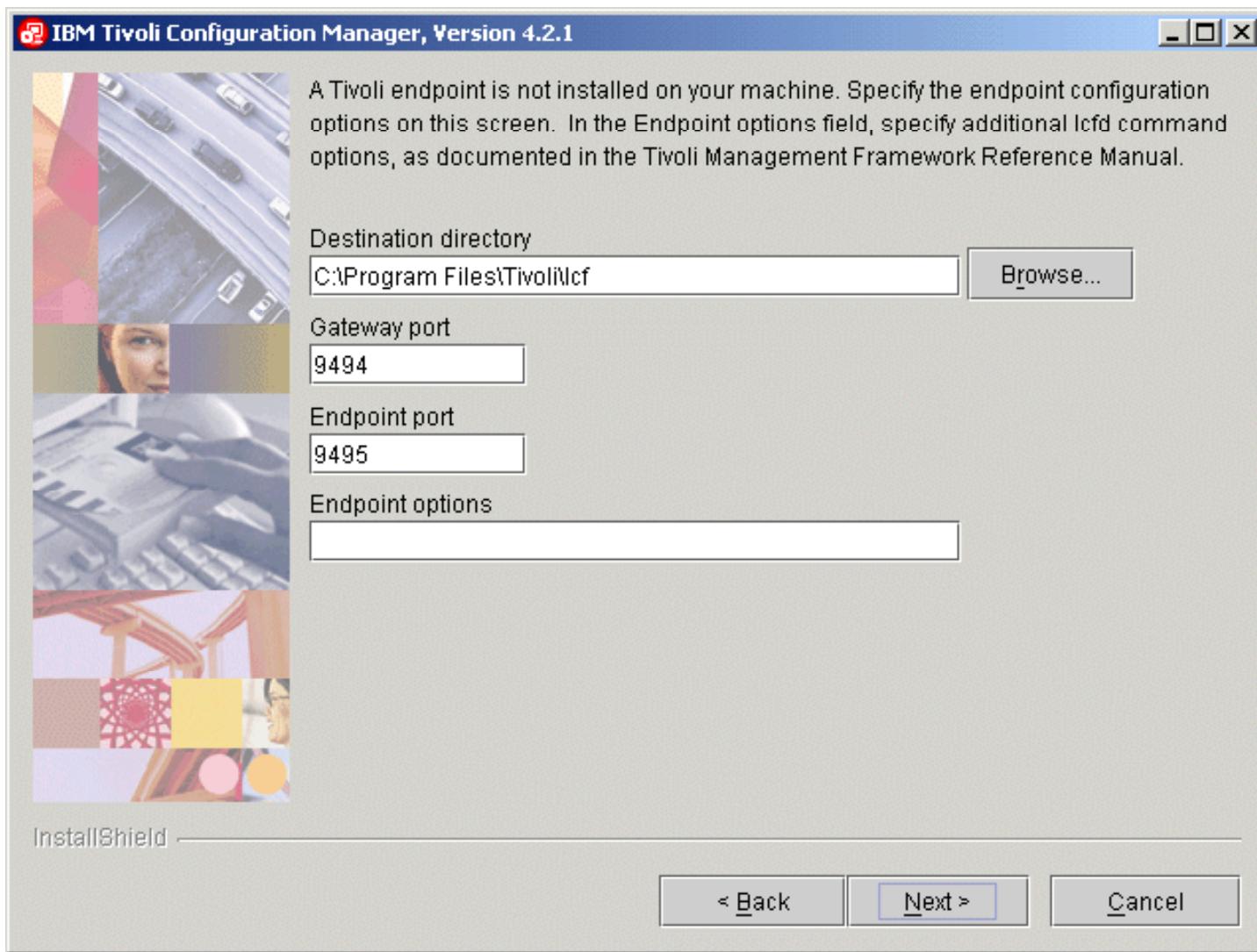
Features:

- Gathers software patch signature files and distributes them to client machines
- Scans clients
- Determines missing patches
- Packages patches
- Builds patch deployment plans
- Distributes required patches to clients

IBM Tivoli Configuration Manager: Screenshot 1



IBM Tivoli Configuration Manager: Screenshot 2





TM

Tool: LANDesk Patch Manager

LANDesk's Patch Manager includes a subscription service that collects and analyzes patches for heterogeneous environments

It scans managed devices to identify application and operating system vulnerabilities

It monitors the status of each install and provides bandwidth throttling, staging, and detailed policy and compliance reporting across a broad range of operating systems

It increases productivity by evaluating systems with active vulnerability scanning

It is used to gain control with a single tool to research, review, and download available patches



TM

LANDesk Patch Manager: Screenshot

The screenshot displays the LANDesk Management Suite interface. The main window title is "LANDesk Management Suite". The menu bar includes File, Edit, View, Tools, Configure, Window, and Help. The toolbar contains icons for Cut, Copy, Paste, Delete, Refresh, and various management functions. The "Core" dropdown is set to "DENNISCORE".

The left pane shows a "Network View" tree with "DENNISCORE (DENNISCORE)" expanded, revealing "Devices", "My devices", "Public devices", and "All devices".

The right pane contains two tables:

- Device View:** Shows a list of devices with columns: Device Name, Type, and DS Name. The entries are:
 - 553648138, BlackBerry/RIM, BlackBerry
 - Dennis, PALM, Palm OS
 - PRECISION-1, 2000 Workstation, Microsoft Windows 2000 Professional
 - PRECISION-2, XP w/rd station, Microsoft Windows XP Professional
- Security and Patch Manager:** Shows a list of spyware items with columns: ID, Severity, Title, Language, Date Published, Repairable, Silent Install, and Auto Fix. The items listed are:

ID	Severity	Title	Language	Date Published	Repairable	Silent Install	Auto Fix
180Solutions	Low	180Solutions	INTL	10/15/2004	Yes	Yes	No
2020Search	Medium	2020Search	INTL	10/15/2004	Yes	Yes	No
2-seek Toolbar	Low	2-seek Toolbar	INTL	10/15/2004	Yes	Yes	No
404search	Low	404search	INTL	10/15/2004	Yes	Yes	No
7adpower	Medium	7adpower	INTL	10/15/2004	Yes	Yes	No
7FaSSt	High	7FaSSt	INTL	10/15/2004	Yes	Yes	No
7search-BrowserA...	High	7search-BrowserAccelerator	INTL	10/15/2004	Yes	Yes	No
AB System Spy	Low	AB System Spy	INTL	10/15/2004	Yes	Yes	No
AccuLoader Dialer	Medium	AccuLoader Dialer	INTL	10/15/2004	Yes	Yes	No
Aconti-Dialer	Medium	Aconti-Dialer	INTL	10/15/2004	Yes	Yes	No
ACsoftware.Narod	High	ACsoftware.Narod	INTL	10/15/2004	Yes	Yes	No
ActualNames	High	ActualNames	INTL	10/15/2004	Yes	Yes	No
AdBar	Medium	AdBar	INTL	10/15/2004	Yes	Yes	No
AdBlaster	High	AdBlaster	INTL	10/15/2004	Yes	Yes	No
AdBreak	High	AdBreak	INTL	10/15/2004	Yes	Yes	No
AdDestroyer	Medium	AdDestroyer	INTL	10/15/2004	Yes	Yes	No
AdGoblin	High	AdGoblin	INTL	10/15/2004	Yes	Yes	No
Adintelligence.Apro... AdLogix	Medium	Adintelligence.AproposToolbar AdLogix	INTL	10/15/2004	Yes	Yes	No
AdPartner	High	AdPartner	INTL	10/15/2004	Yes	Yes	No



TM

Tool: ConfigureSoft Enterprise Configuration Manager (ECM)

ECM centralizes and automates the monitoring, managing and auditing of hardware and software configurations across Windows, UNIX, and Linux platforms

It automatically discovers new systems and tracks configuration changes at scheduled intervals to ensure the availability of the latest patch information is available

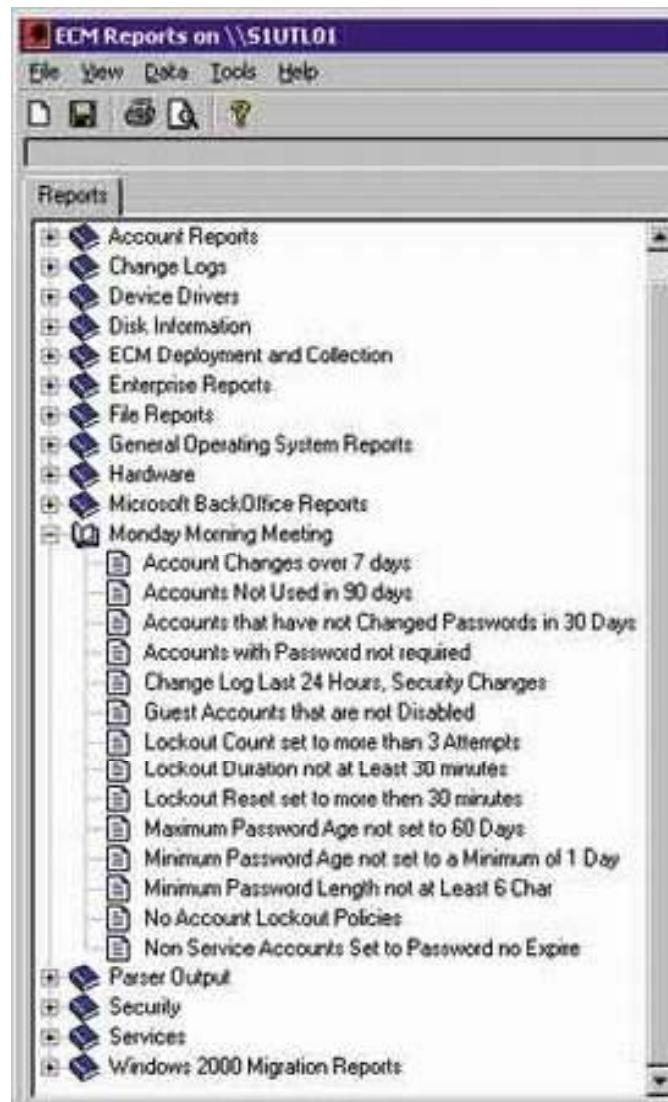
Features:

- Vulnerabilities assessment and remediation
- Regulatory & operational compliance
- Configuration management & control
- Change management
- Risk prevention and security management
- System optimization



TM

ConfigureSoft Enterprise Configuration Manager (ECM): Screenshot





Tool: BladeLogic Configuration Manager

BladeLogic Configuration Manager is a component of the BladeLogic Operations Manager suite of data center automation products

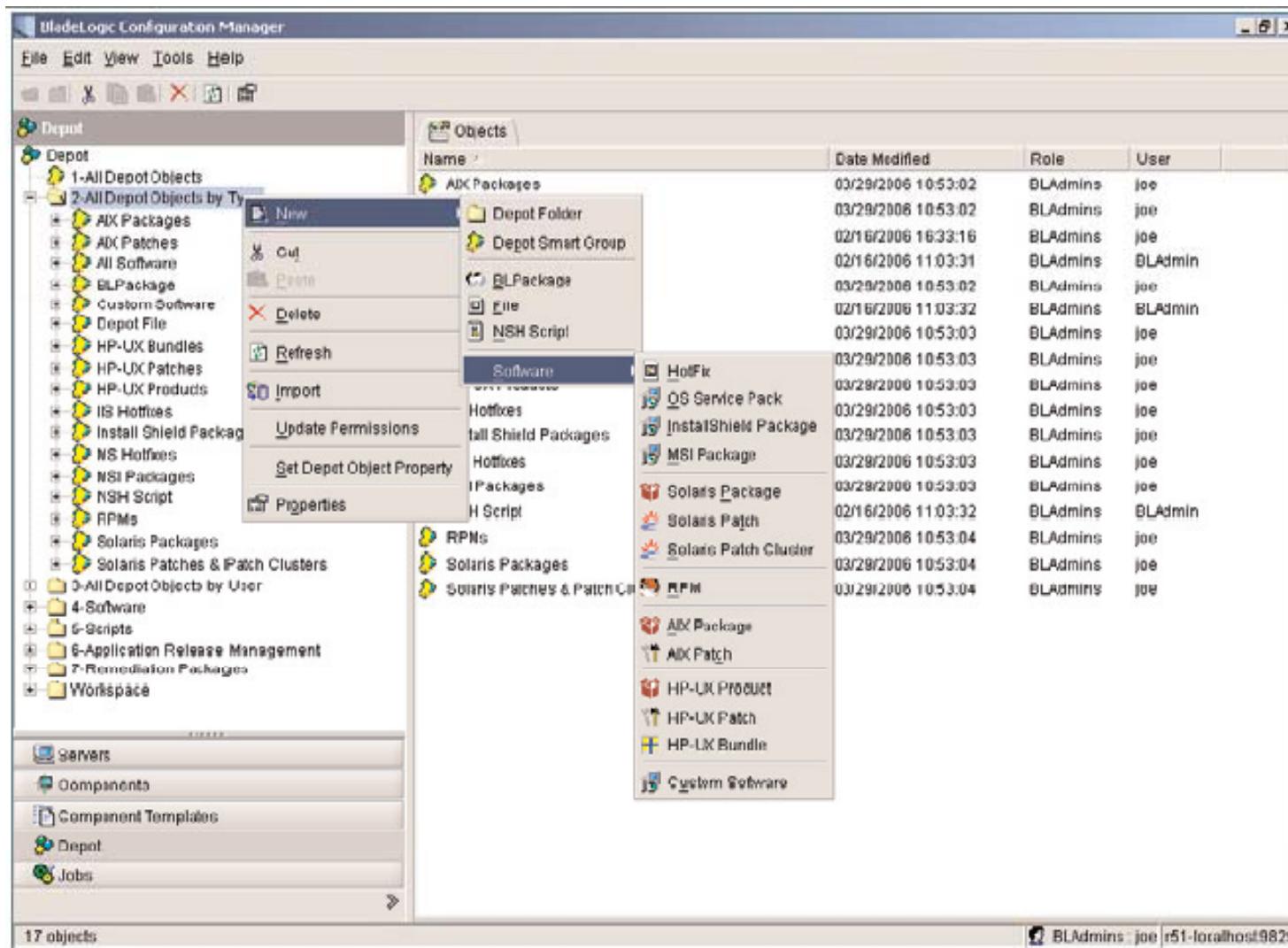
It features a cross-platform command line interface that supports a single-sign on using a range of authentication protocols

It supports a policy-based approach whereby changes are applied to a policy, and then synchronized with the target servers

All user communication is encrypted, and all user actions are logged and can be authorized based on a user's role

It allows IT organizations to monitor, patch, configure, and update servers across platforms and data centers

BladeLogic Configuration Manager: Screenshot





Tool: Microsoft Baseline Security Analyzer (MBSA)

Microsoft baseline security analyzer determines critical updates and the required updates on the target computer

It scans for common security mis-configuration errors on target computers

It supports two interface for scanning:

- GUI Scan (Mbsa.exe)
- Command Line Interface (Mbsacli.exe)

MBSA: Scanning Updates in GUI Mode

MBSA defines scanning options and displays the results of the security scan in the MBSA window

It scans and reports on updates designated as critical security updates by the Windows Update site

Procedure:

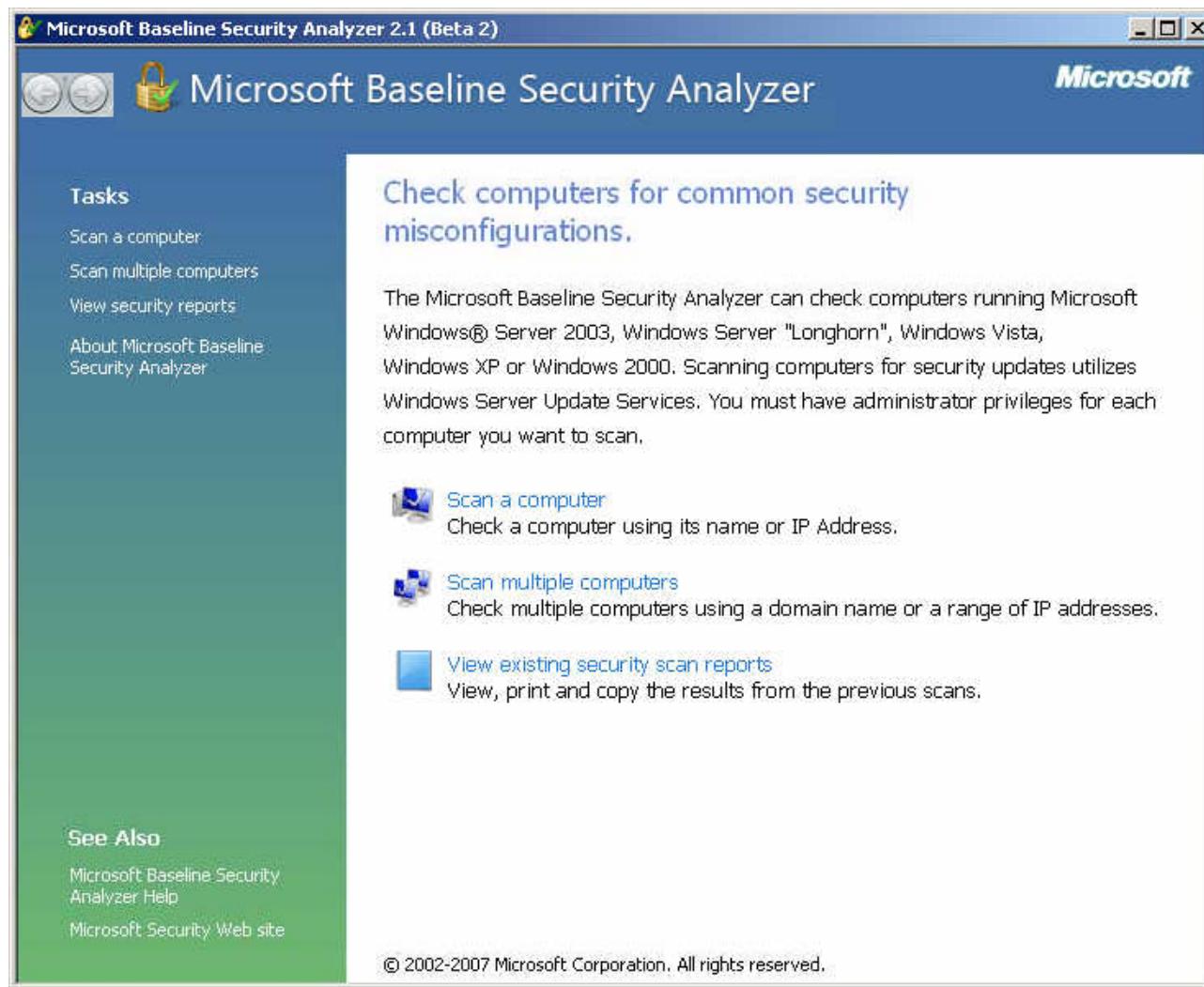
- Open MBSA
- Enable the check For security updates option
- Scan completion display XML file for the respective computer





TM

MBSA: Screenshot



MBSA: Scanning Updates in Command-line Version

The MBSA command line interface supports two types of scan namely:

MBSA-style
scan

```
•mbsacli [/c|/i|/r|/d domainname|ipaddress|ipaddressrange]
[/n option] [/sus SUS server|SUS filename] [/s level]
[/nosum] [/nvc] [/o filename] [/e] [/l] [/ls] [/lr report
name] [/ld report name] [/v] [/?] [/qp] [/qe] [/qr] [/q]
[/f] [/unicode]
```

HFNetChk-
style scan

```
•mbsacli /hf [-h hostname] [-fh filename] [-i ipaddress] [
-fip filename] [-r ipaddressrange] [-d domainname] [-n] [-sus
SUS server|SUS filename] [-fq filename] [-s 1] [-s 2] [
-nosum] [-sum] [-z] [-v] [-history level] [-nvc] [-o option]
[-f filename] [-unicode] [-t] [-u username] [-p password] [
-x] [-?]
```



TM

Tool: QChain

Qchain allows to install multiple security updates

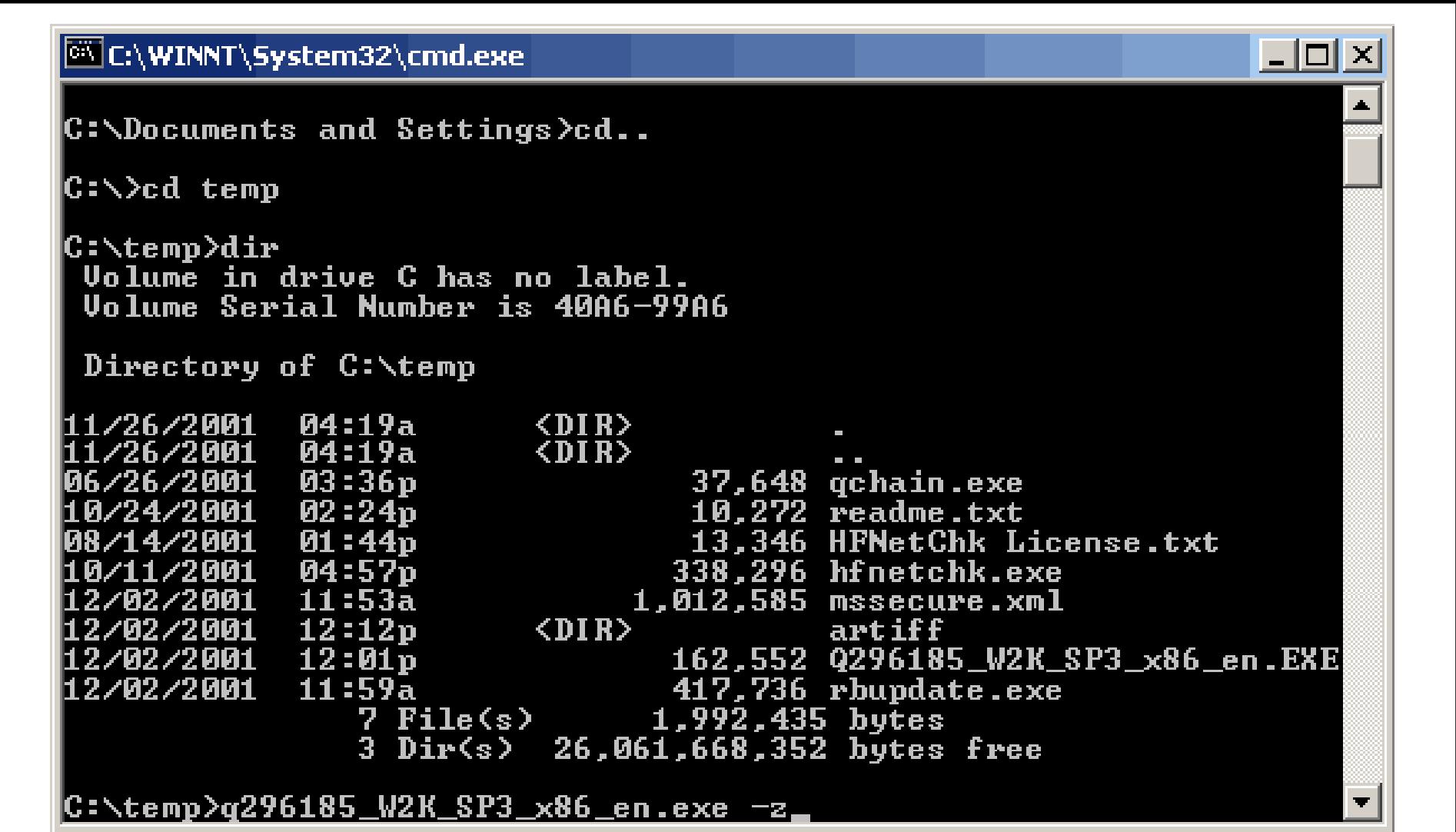
It evaluates the drivers, DLLs, and executable files updated by each security update

It creates a batch file for the security update installation

Batch file installs each security update with:

- **-z** switch to prevent reboots after each security update installation
- **-m** switch to enable unattended installs

Qchain: Screenshot 1



The screenshot shows a Windows Command Prompt window with the title bar "C:\WINNT\System32\cmd.exe". The command history and output are as follows:

```
C:\Documents and Settings>cd..
C:\>cd temp
C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is 40A6-99A6

Directory of C:\temp

11/26/2001  04:19a      <DIR>          .
11/26/2001  04:19a      <DIR>          ..
06/26/2001  03:36p            37,648 qchain.exe
10/24/2001  02:24p            10,272 readme.txt
08/14/2001  01:44p            13,346 HFNetChk License.txt
10/11/2001  04:57p            338,296 hfnetchk.exe
12/02/2001  11:53a           1,012,585 mssecure.xml
12/02/2001  12:12p      <DIR>          artiff
12/02/2001  12:01p            162,552 Q296185_W2K_SP3_x86_en.EXE
12/02/2001  11:59a            417,736 rbupdate.exe
                           7 File(s)   1,992,435 bytes
                           3 Dir(s)  26,061,668,352 bytes free

C:\temp>q296185_W2K_SP3_x86_en.exe -z_
```



TM

Qchain: Screenshot 2

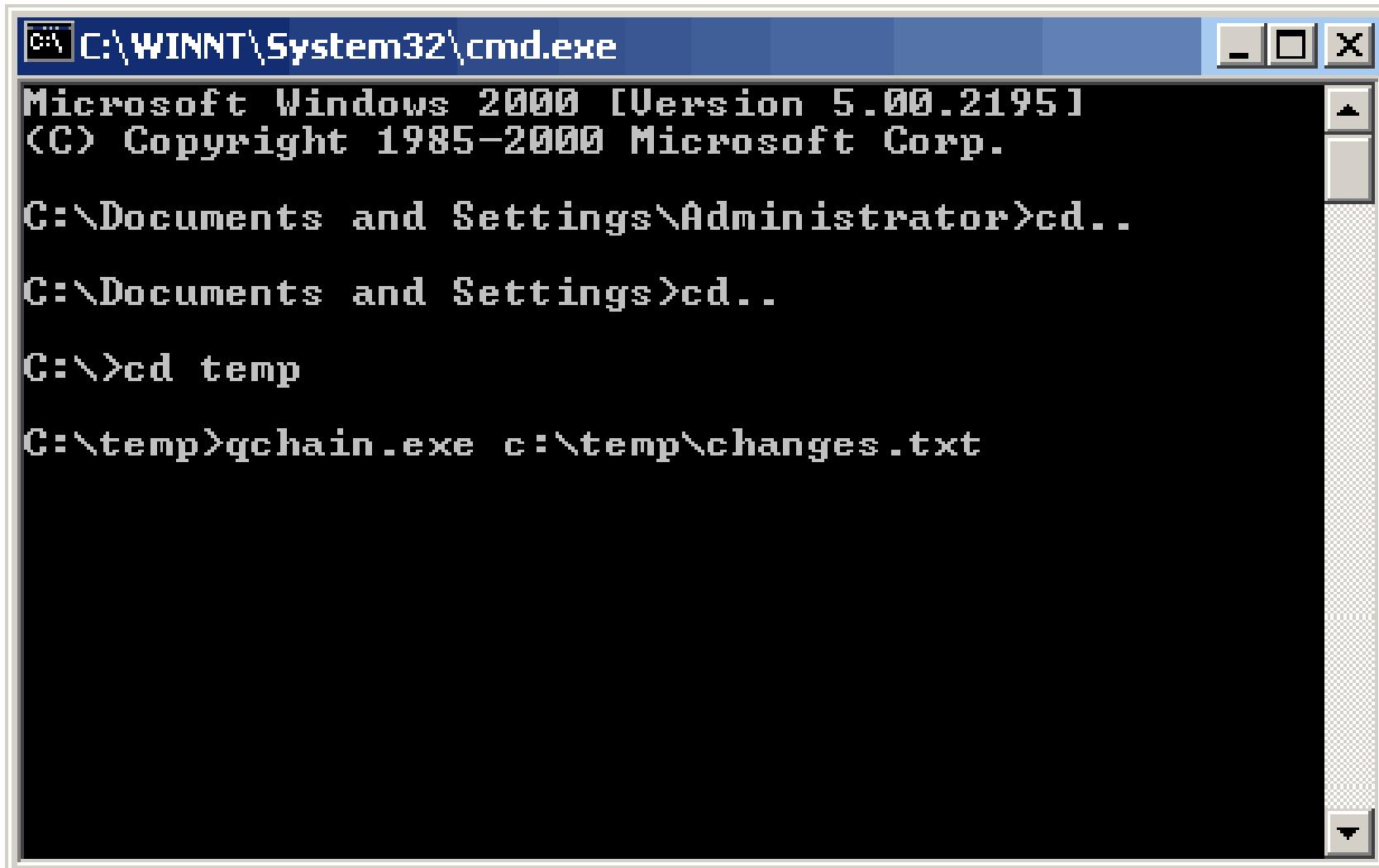
```
C:\WINNT\System32\cmd.exe
C:\Documents and Settings\Administrator>cd..
C:\Documents and Settings>cd..
C:\Documents and Settings>cd..
C:\>cd temp
C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is 40A6-99A6

Directory of C:\temp

11/26/2001  04:19a    <DIR>          .
11/26/2001  04:19a    <DIR>          ..
06/26/2001  03:36p            37,648  qchain.exe
10/24/2001  02:24p            10,272  readme.txt
08/14/2001  01:44p            13,346  HFNetChk License.txt
10/11/2001  04:57p            338,296 hfnetchk.exe
12/02/2001  11:53a           1,012,585 mssecure.xml
                           5 File(s)   1,412,147 bytes
                           2 Dir(s)  26,086,359,010 bytes free

C:\temp>
```

Qchain: Screenshot 3



A screenshot of a Microsoft Windows 2000 Command Prompt window. The title bar reads "C:\WINNT\System32\cmd.exe". The window displays the following text:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>cd..
C:\Documents and Settings>cd..
C:\>cd temp
C:\temp>qchain.exe c:\temp\changes.txt
```



Tool: BigFix Enterprise Suite (BFS)

BigFix Enterprise Suite platform provides patch management solution for distributed and multiplatform networks

Roll back feature helps in securing the system in case of patches that misfire

It enables audit trial of every action and step taken on each computer during the patch management process

BigFix Enterprise Suite (BFS): Screenshot 1

The screenshot shows the BigFix Enterprise Console interface. The main window displays a list of 'All Relevant Fixlet Messages (49)' under the heading 'Fixlet: MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - MDAC 2.80 - Windows 2000/XP'. The list includes several critical vulnerabilities, such as MS06-015, MS06-014, and MS06-013. The details pane below shows a summary of the selected fixlet, including its severity (Critical), a brief description, and links to comments, relevant computers, and action history.

Fixlet: MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - MDAC 2.80 - Windows 2000/XP

Severity: Critical

Description: Microsoft has released a patch eliminating a newly-discovered, privately-reported security vulnerability in the Microsoft Data Access Components (MDAC) Function. If a user is logged on with administrative rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Note: After downloading and installing this patch, affected computers will no longer be susceptible to these vulnerabilities.

Note: Affected computers may report back as 'Pending Restart' once the patch has run successfully, but will not report back their final status until the computer has been restarted.

Note: Microsoft has announced that the update for this issue may be included in a future Update Rollup.

BigFix Enterprise Suite (BFS): Screenshot 2

The screenshot shows the 'Computer Status' window of the BigFix Enterprise Suite. The left pane displays a tree view with 'All Computers (101)' selected, showing nodes for 'By Active Directory' and 'By Retrieved Properties'. The main pane lists computer details:

Name	User Name	OS	CPU
Aberlard-1238090	Nelson Muntz	Win2000 5.0.2...	1615 Mhz Per
Adams-1604070	Sideshow Mel	WinME Initial.7...	1994 Mhz Per
Ambrose-1143553	Luann Van Houten	Win2000 5.0.2...	1994 Mhz Per
Anaximander-11...	Jebediah Spring...	Win98 Initial.67...	1787 Mhz Per
Ansem-1124327	Nelson Muntz	WinME Initial.7...	1812 Mhz Per
Antisthenes-127...	Luann Van Houten	Win98 Initial.67...	1994 Mhz Per
Aquinas-1226249	Ralph Wiggum	WinXP 5.1.2600	1596 Mhz Per
Aristotle-1985909	Jackie Bouvier	Win2000 5.0.2...	1596 Mhz Per
Arthur-1974628	Jasper	Win2000 5.0.2...	1812 Mhz Per

The right pane contains buttons for 'Remove', 'Send Refresh', 'Edit Settings', and 'Edit Management Rights'. Below the main pane are tabs for 'Relevant', 'Actions', 'History', 'Properties', 'Settings', and 'Management Rights'. The 'Management Rights' tab is active, showing a list of security patches:

Name	Category	Download Size	Source	Source ID
MS01-002: "Unchecked Buffer" in PowerPoint File Parse...	Security Update	809 KB	Microsoft	Q285978
MS02-008: XML Core Services 2.6 XMLHTTP Control (M...	Security Hotfix	367 KB	Microsoft	Q318202
MS02-021: E-mail Editor Flaw Could Lead to Script Exec...	Security Update	2.00 MB	Microsoft	Q321804
MS02-025: CORRUPT PATCH - Exchange 2000	Security Hotfix	Open	Microsoft	Q320436
MS02-032: 26 June 2002 Cumulative Patch for Windows...	Security Hotfix	Take Default Action	Microsoft	Q320920
MS02-044: Unsafe Functions in Office Web Components...	Security Update	Copy	Microsoft	Q328130
MS02-045: CORRUPT PATCH - Windows XP	Security Hotfix	Select All	Microsoft	Q326830
MS02-050: Certificate Validation Flaw Could Enable Ident...	Security Hotfix	483 KB	Microsoft	Q329115
MS02-053: Buffer Overrun in SmartHTML Interpreter Cou...	Security Hotfix	2.30 MB	Microsoft	Q324096
MS02-054: Unchecked Buffer in File Decompression Fun...	Security Update	286 KB	Microsoft	Q329048
MS02-055: CORRUPT PATCH - Windows XP	Security Hotfix	694 KB	Microsoft	Q323255
MS02-062: October 2002 Cumulative Patch for Internet I...	Security Hotfix	1.13 MB	Microsoft	Q327696
MS02-068: Cumulative Patch for Internet Explorer 6	Security Hotfix	2.43 MB	Microsoft	Q324929
MS02-072: Unchecked Buffer in Windows XP Gold Shell	Security Hotfix	282 KB	Microsoft	Q329390
MS99-030: Office 97 ODBC Vulnerabilities	Security Hotfix	4.65 MB	Microsoft	<unspecified>

At the bottom of the window are buttons for 'Open' and 'Take Default Action'.



TM

Tool: Shavlik NetChk Protect

Shavlik NetChk protect is a patch management solution for larger networks and organizational units

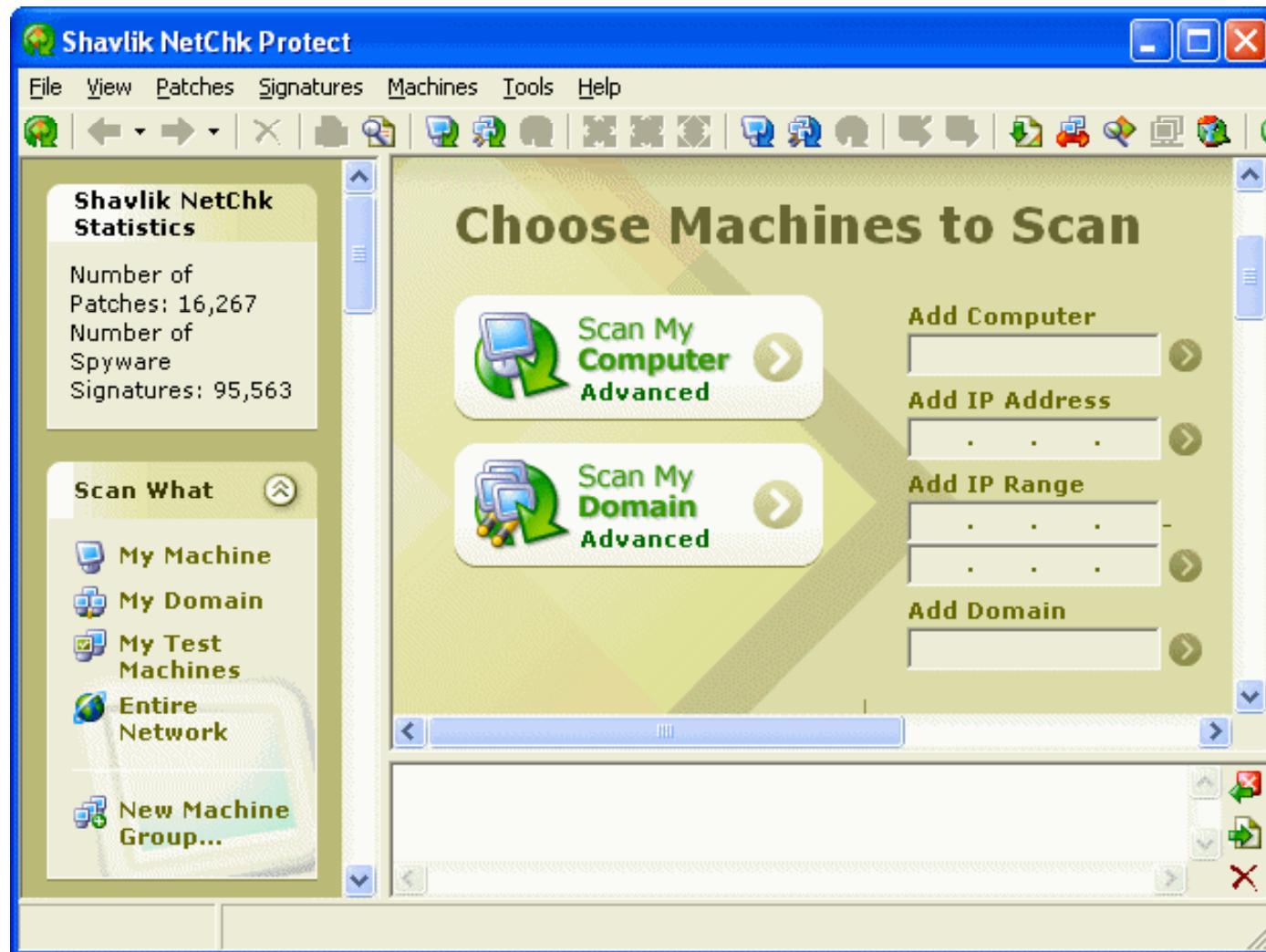
Features:

- Drag-n-Drop patch management interface controlled by the user enables scanning of the required groups
- Security configuration management mitigates organizational costs and provides the security associated with the expensive breaches
- It automates the platforms and products such as Windows NT, XP,2000, etc

Benefits:

- Performs scheduled scans
- Uses options such as Command line scanning and scanning and deployment with SQL server database

Shavlik NetChk Protect: Screenshot





TM

Tool: PatchLink Update

PatchLink Update is a patch and vulnerability solution for large networks

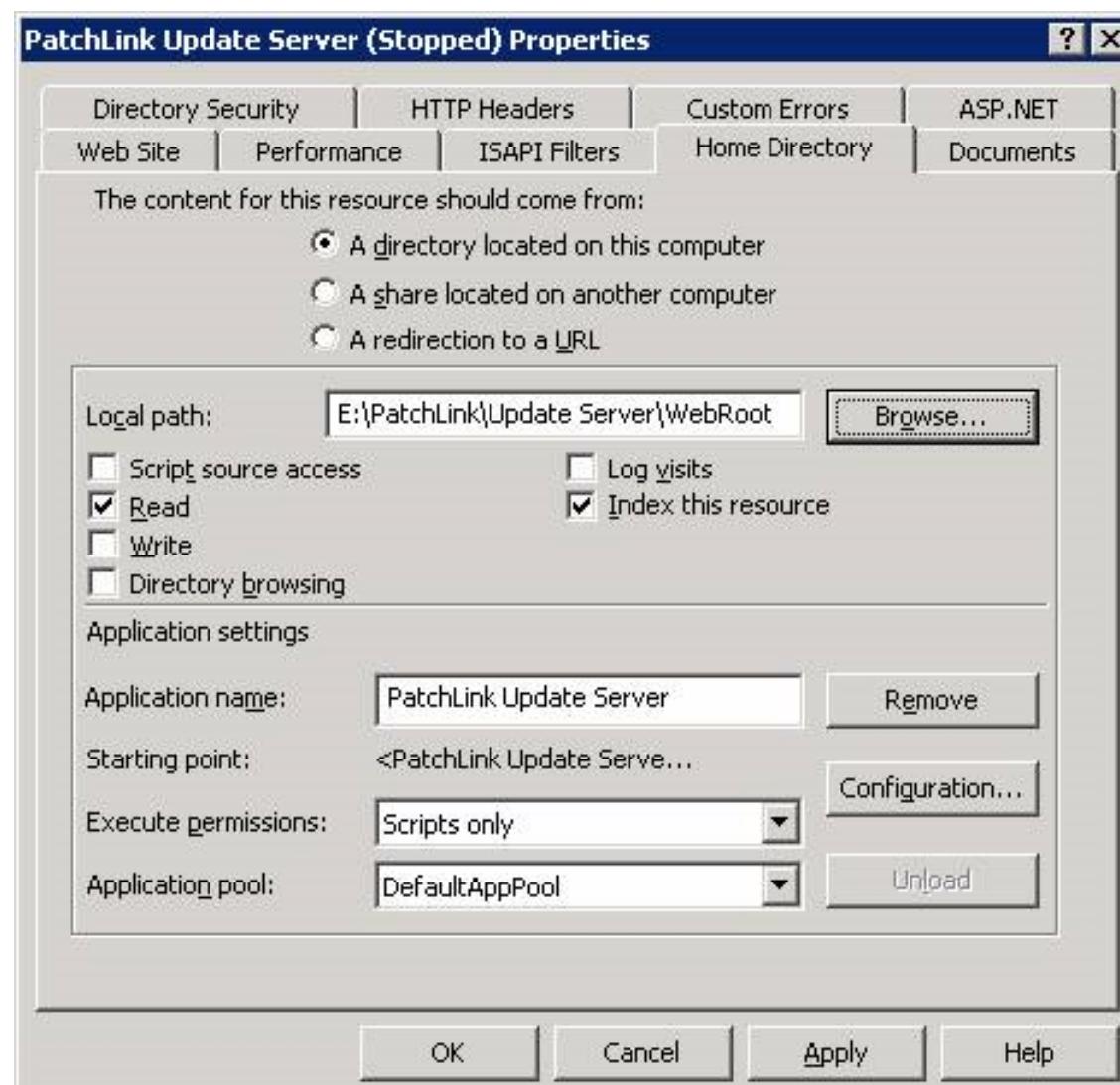
It scans networks for security holes using fingerprint technology

It translates security policies into automated and continuous protection against network vulnerabilities

Features:

- Customized subscription notifications to include the required platforms and languages
- Improved transaction/query efficiency that increases performance and scalability
- Proxy server authentication that increases deployment security

PatchLink Update: Screenshot





TM

Tool: SecureCentral PatchQuest

SecureCentral PatchQuest is a web-based patch management software that manages and distributes security patches across various platforms

Four stages in working:

- System addition & discovery
- Patch assessment or scanning
- Patch download and deployment
- Reporting

Features:

- Flexible modes of operation
- Web-based administration console for universal secure-access to data views and configurations
- Cross-platform product installation
- Array of reports to facilitate quick access to the data required



TM

SecureCentral PatchQuest: Screenshot 1

Screenshot of the SecureCentral PatchQuest interface showing a system scan result.

Actions:

- Scan System Now
- Configure System Info
- Add/Edit User Comment
- View Scan Result
- Update Agent Version

Reports:

- No Tasks Scheduled
- Task History
- Compare Scan Results

Bookmarks:

- Dec_rel
- nonsec_upd...

Scan Result: sd-test3

Product Summary:

Product Name	Service Packs	Available Patches	Missing Patches	Informational Item	Obsolete Patches
All	44	66	12	4	26
Windows 2000 Professional SP4 (OS)	1	56	10	2	21
Excel 2000 Gold	5	1	0	0	0
Internet Explorer 6. Gold	2	1	0	0	0
MDAC 2.6 SP2	1	1	0	0	2
MSXML 2.6 SP2	2	0	0	0	0
MSXML 3.0 SP7	1	0	0	0	0
MSXML 4.0 SP2	1	0	1	0	1
MSXML 6.0 Gold	1	0	1	0	1
Office 2000 Gold	15	3	0	0	0
Outlook 2000 Gold	15	0	0	0	0
Outlook Express 6.0 Gold	2	0	0	0	1
PowerPoint 2000 Gold	10	0	0	0	0
SQL Server 2000 Gold	10	3	0	1	0
Windows Media Player 6.4 for Windows 2000 SP4	1	1	0	0	0
Word 2000 Gold	6	0	0	1	0
DirectX 7.0 Gold	1	0	0	0	0

Agent Status: PatchQuest Agent, Running, Up-to-date

Patch List:

Patch Status	Bulletin ID	Patch Name	Installation Status	Download Status	Severity
Green	MSRT-001	New Windows-KB890830-ENU.exe	NA	Download	N
Green	MS99-044	x19sp4pu4.exe	NA	Download	U
Green	MS99-030	Jetcpkq.exe	NA	Download	U
Green	MS06-078	New WindowsMedia6-KB925398-x86-ENU....	NA	Download	C
Yellow	MS06-077	New Windows2000-KB926121-x86-ENU.E....	NA	Download	I
Red	MS06-071	msxml4-KB927978-enu.exe	NA	Download	C
Red	MS06-074	msxml6-KB927977-enu-x86.exe	NA	Download	C
Red	MS06-070	Windows2000-KB924270-x86-ENU.E....	NA	Download	C
Red	MS06-068	Windows2000-KB920213-x86-ENU.E....	NA	Download	C

© 2006 AdventNet Inc

Server responded in 1863 milliseconds.

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited



TM

SecureCentral PatchQuest: Screenshot 2

secure | central™
PatchQuest

Home Systems System Groups Patch Information Patch Groups Reports Settings Support

Quick Search Update DB Add System Scan System Deploy Patches Deploy Service Packs Recent Tasks

Systems
All Systems Windows Red Hat Debian

Agent Update Status
Windows Linux

Bookmarks + No Bookmark Available. [Add new?](#)

Scan Result » SD-TEST3

Deploy Download Undeploy Add To Patch Group Scan Now Export Print Help

Search None like Go Entries per page 25 Edit Column

Showing 1 to 25 of 60

Patch Status	Bulletin ID	Patch Name	Title	Installation Status	Download Status	Severity	Superseded By	Views
<input type="checkbox"/>	MS05-037	New IE5.01-KB903235-x86-ENU.exe	Vulnerability in JView Profiler Could Allow Remote Code Execution (903235)	NA			NA	
<input type="checkbox"/>	MS05-036	New Windows2000-KB901214-x86-ENU.exe	Vulnerability in Microsoft Cluster Management Module Could Allow Remote Code Execution (901214)	NA			NA	
<input type="checkbox"/>	MS05-032	Windows2000-KB890046-x86-ENU.EXE	Vulnerability in Microsoft Agent Could Allow Spoofing (890046)	NA			NA	
<input type="checkbox"/>	MS05-031	StepByStepInteractiveTraining-KB898458-x86-ENU.exe	Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (898458)	NA			NA	
<input type="checkbox"/>	MS05-027	Windows2000-KB896422-x86-ENU.EXE	Vulnerability in Server Message Block Could Allow Remote Code Execution (096422)	NA			NA	
<input type="checkbox"/>	MS05-011	Windows2000-KB885250-x86-ENU.EXE	Vulnerability in Server Message Block Could Allow Remote Code Execution (885250)	NA			NA	
<input type="checkbox"/>	MS05-008	Windows2000-KB890047-x86-ENU.EXE	Vulnerability in Windows Kernel Could Allow Remote Code Execution (890047)	NA			NA	
<input type="checkbox"/>	MS05-003	Windows2000-KB871250-x86-ENU.EXE	Vulnerability in the Indexing Service Could Allow Remote Code Execution (871250)	NA			NA	
<input type="checkbox"/>	MS05-002	Windows2000-KB891711-x86-ENU.EXE	Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution (891711)	NA			MS05-018	
<input type="checkbox"/>	MS05-001	Windows2000-KB890175-x86-ENU.EXE	Vulnerability in HTML Help Could Allow Code Execution (890175)	NA			MS05-026	
<input type="checkbox"/>	MS04-044	Windows2000-KB885835-x86-ENU.EXE	Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (885835)	NA			NA	
<input type="checkbox"/>	MS04-043	Windows2000-KB873339-x86-ENU.EXE	Vulnerability in Hyper-Terminal Could Allow Code Execution (873339)	NA			NA	
<input type="checkbox"/>	MS04-041	Windows2000-KB885836-x86-ENU.EXE	Vulnerability in WordPad Could Allow Code Execution (885836)	NA			NA	

© 2005 AdventNet Inc.

Server responded in 125 milliseconds.

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited



TM

Tool: Patch Authority Ultimate

Patch authority ultimate is ScriptLogic's comprehensive and enterprise-class patch management solution

It prevents attacks and exploits through centralized control of updates on all Windows desktops and servers

Benefits:

- Leading patch database and scan engine
- Selection, distribution, deployment, and reporting are all part of this comprehensive solution
- Management reports show overall patch status across the network
- Centralized management of patch policy and status for all computers, local and remote, on the LAN and across the Internet
- A baseline of patches can be created to establish a "secure" machine
- Enhanced security with central management of service status, configuration, logon accounts, and scheduled task configuration

Patch Authority Ultimate: Screenshot

The screenshot displays the 'Patch Authority Ultimate' application window. On the left, a sidebar includes 'Patch Authority Ultimate Statistics' (Number of Patches: 24,458), 'Scan What' (My Machine, My Domain, My Test Machines, Entire Network, New Machine Group...), 'Favorites' (New Patch Favorite...), 'Today's Items' (8:41:43 AM (1), 8:39:59 AM (1)), and 'Recent Items' (8/6/2007 11:55:05 AM (6), 8/3/2007 8:40:00 AM (6), 8/3/2007 8:22:05 AM (1)). The main area shows a tree view under 'XPCCLIENT4' with 'Executive Summaries' and 'Summary by Patch'. A large table lists patches, and a detailed view for 'Missing Patch Q935840 MS07-031' is shown.

Type	QNumber	Item	Deployment
Missing Patch	Q935840	MS07-031	Wir
Missing Patch	Q935839	MS07-035	Wir
Missing Patch	Q933566	MS07-033	Inte
Missing Patch	Q932168	MS07-020	Wir
Missing Patch	Q931784	MS07-022	Wir
Missing Patch	Q931261	MS07-019	Wir
Missing Patch	Q930178	MS07-021	Wir
Missing Patch	Q929969	MS07-004	Wir
Missing Patch	Q929123	MS07-034	Wir
Missing Patch	Q928843	MS07-008	Wir
Missing Patch	Q928255	MS07-006	Wir
Missing Patch	Q927802	MS07-007	Wir
Missing Patch	Q927779	MS07-009	MD
Missing Patch	Q926436	MS07-011	Wir
Missing Patch	Q926255	MS06-075	Wir

Patch Details:
 Status: Missing Patch [Install Patch](#)
 Vendor Severity: Critical [Add...](#)
 Criticality: Not Set [Add...](#)
 CVEID: CVE-2007-2218
 Patch Download Status: English [Download](#)
 Comments: None [Add/Edit Comment...](#)

Windows XP Professional Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)

File version is less than expected: [\\192.168.11.131\C\$\WINDOWS\system32\SCHANNEL.DLL, 5.1.2600.2180 < 5.1.2600.3126]

Bulletin ID: [MS07-031](#) Microsoft Knowledge Base Article: [Q935840](#)

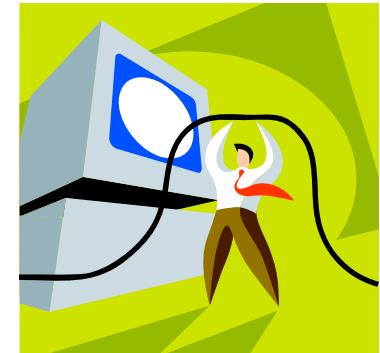
Summary
 This critical security update resolves a privately reported vulnerability in the Secure Channel (Schannel) security package in Windows. The Schannel security package implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Internet standard authentication protocols. This vulnerability could allow remote code execution if a user clicked a specially crafted link.

Tool: ZENworks Patch Management

ZENworks Patch Management is a piece of automated patch management software

It can be used to protect your network from the viruses by automating the process of discovering security alerts, retrieving the patches, and deploying the right ones to the right machines at the right time to prevent problems

It provides patches for more than 40 different operating systems, applications, and software



ZENworks Patch Management: Screenshot

The screenshot shows the Novell ZENworks PatchLink Update interface. At the top, there's a navigation bar with links to Home, Reports, Inventory, Packages, Computers, Groups, Users, Options, Help, and a timestamp of 4/2/2004 11:14:23 AM (GMT-07:00). A large banner on the left side lists several links: Get support and the latest information about patches..., What is PatchLink Update?, New Users Start Here, Help Info, and Known Issues & Resolutions. On the right side, a detailed view of a Microsoft Security Bulletin MS04-009 is displayed, including the date released (March 10, 2004), severity (Important), date released (March 9, 2004), systems affected (Office XP SP2, Office 2002 SP2), and recommendation (Customers should install the patch at [dropdown]). Below this, a section titled "Comprehensive Graphical Assessments:" features a pie chart titled "Patch Status for all Reports". The chart shows the following distribution: 25.0% in red, 66.9% in green, and 8.1% in orange. A dropdown menu titled "Select to Change Graph:" offers options: Patch Status for all Computers, Patch Status for all Reports (which is selected), Status for all Computers, and Baseline Status for all Groups.

Novell ZENworks®

PATCHLINK

Server Time: 4/2/2004 11:14:23 AM (GMT-07:00)

Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help |

Get support and the latest information about patches....

What is PatchLink Update?
Select this link to see an overview of PatchLink Update including its features and benefits...

New Users Start Here
If you are new to PatchLink Update, select this link to see how to get up and running fast...

Help Info
Select this link for full comprehensive help documentation about PatchLink Update...

Known Issues & Resolutions
Select this link to see a list of known issues and release notes about this version of the PatchLink Update Server.

Comprehensive Graphical Assessments:

Patch Status for all Reports

Status	Percentage
Red	25.0%
Green	66.9%
Orange	8.1%

patchlink

Select to Change Graph:

- Patch Status for all Computers
- Patch Status for all Reports**
- Status for all Computers
- Baseline Status for all Groups



Tool: Ecora Patch Manager

Ecora Patch Manager automates system discovery, patch assessment, and patch installation on workstations and servers

Features:

- Agent-less or optionally agent-based
- Views missing patches by systems, applications, specific patches, or according to your policy
- Patches any Windows application Microsoft supports, other companies' Windows-based patches, or patches for home grown applications
- Has automated patch roll-back on one or more machines
- Logically groups systems for ease of management
- Scheduled patch deployment

Ecora Patch Manager: Screenshot 1

The screenshot shows the Ecora Patch Manager application window. On the left is a tree view of system nodes under 'Roots'. A context menu is open over a node labeled 'ECORAQATIMPE'. The menu options are: Select All, Unselect All, Select All Missing Patches for Push, Select All Undetermined Patches for Push, Select All Warning Patches for Push, and Select All Available Patches for Push. The main pane displays a table of patches for 'System: TEMP'. The columns are: Push, Rollback, Installed, Risk, Application, Patch Name, Hotfix, Bulletin, and Status. The table contains several rows of patch information, including service packs for Internet Explorer and Windows, and Media Player patches. At the bottom right of the main pane are buttons for Manage Notes, Approve Push, Comment, Ignore Patch, and Approve Rollback.

All	IE	HS	MOAC 2.0	SQL 2000	OS	Media Player	
System: TEMP							
Push	Rollback	Installed	Risk	Application	Patch Name	Hotfix	Bulletin
<input checked="" type="checkbox"/>		Undetermined	MEDIUM	OS	W2K_MS02_064	327522	MS02_064
<input type="checkbox"/>		Missing Service Pack	IE	Internet Explorer 6 SP1	Service Pack	Service Pack	Service Pack
<input type="checkbox"/>		Missing Service Pack	OS	Windows 2000 Service Pack 4	Service Pack	Service Pack	Service Pack
<input type="checkbox"/>		Missing Patch	LOW	0326886_W2K_SP4_086.exe	326886	MS02_042	
<input type="checkbox"/>		Missing Patch	MEDIUM	0811114_W2K_SP4_086.exe	811114	MS03_018	
<input type="checkbox"/>		Missing Patch	MEDIUM	mm320920_04.exe	320920	MS02_032	
<input type="checkbox"/>		Missing Patch	MEDIUM	0329115_W2K_SP4_086.exe	329115	MS02_050	
<input type="checkbox"/>		Missing Patch	MEDIUM	0810033_W2K_SP4_086.exe	810033	MS03_001	
<input type="checkbox"/>		Missing Patch	MEDIUM	0811493_W2K_SP4_086.exe	811493	MS03_013	

Ecora Patch Manager: Screenshot 2

Missing Patches - Microsoft Internet Explorer

File Edit View Favorites Tools Help

ecora Missing Patches

Print Report...

Page 1 of 2 1-30 of 46 items shown

Patch	Risk	Product Name	System	Note	OS Name	Scan Time
280380		SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
304404		Windows Media Player 6.4 For Windows 2000 Windows Media Player 6.4 For Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
242479		Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
823559	▲ MEDIUM	Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\BOSTON	[P]	Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
280419		Windows Media Player 6.4 For Windows 2000 Windows Media Player 6.4 for Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
308567		Windows Media Player 6.4 For Windows 2000 Windows Media Player 6.4 for Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
300635		MDAC 2.6 MDAC 2.6 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
823980	■ HIGH	Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\BOSTON	[P]	Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
298012	● LOW	SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
296138	▲ MEDIUM	Windows Media Player 6.4 for Windows 2000 Windows Media Player 6.4 For Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
306908		SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
306908		SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
263968		SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
824105		Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\BOSTON	[P]	Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
299717	● LOW	SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
320920	▲ MEDIUM	Windows Media Player 6.4 for Windows 2000 Windows Media Player 6.4 For Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
304404		Windows Media Player 6.4 For Windows 2000 Windows Media Player 6.4 For Windows 2000 Gold	ECORAQA\NEWYORK		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
242479		Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\NEWYORK		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
256052	● LOW	SQL Server 7.0 SQL Server 7.0 Gold	ECORAQA\NEWYORK		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
823559	▲ MEDIUM	Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\NEWYORK	[P]	Windows 2000 Advanced Server	10/16/2003 4:35:17 PM



TM

Tool: Service Pack Manager

Service Pack Manager enables system administrators to fix security vulnerabilities and stability problems in Windows NT/2000/XP/2003 and additional Microsoft products

It allows to remotely detect, track, monitor, and install Windows NT/2000/XP/2003 Service Packs and Hotfixes on the enterprise networks from a central console

Remote inventory, research, and deployment of the security vulnerabilities patches and stability updates make Service Pack Manager a highly cost-effective tool when used on the enterprise LANs and WANs

The installation status of hundreds of hotfixes can be detected quickly on any number of remote computers

It makes the task of maintaining security of the large networks viable

Service Pack Manager: Screenshot





TM

Tool: Altiris Patch Management Solution

Altiris Patch Management Solution software proactively manages patches and software updates by automating the collection, analysis, and delivery of patches across your enterprise

It helps you to decrease the costs involved in delivering patches throughout your enterprise and integrates with Altiris Recovery Solution for stable-state rollback

It provides improved functionality in the analysis, collection, and distribution of OS and application updates

It improves business continuity and accelerates IT systems' security by reducing the need for extended patch test cycles

Altiris Patch Management Solution: Screenshot 1

The screenshot shows the Altiris Console interface in Microsoft Internet Explorer, version 6.0.5287. The title bar reads "Altiris Console - Microsoft Internet Explorer". The main menu includes File, Edit, View, Favorites, Tools, and Help. The toolbar includes Back, Forward, Stop, Refresh, Search, Favorites, Media, and Links. The address bar shows the URL "http://localhost/Altiris/NS/Console.aspx". The Altiris logo is in the top right corner.

The navigation bar at the top has tabs: Getting Started, Tasks, Resources, Reports, Configuration, Shortcuts, Incidents. The Configuration tab is selected. On the left, a sidebar tree view shows:

- Configuration
 - Altiris Agent
 - Resource Settings
 - Server Settings
 - Solutions Settings
 - Incident Management
 - Carbon Copy
 - Recovery Solution
 - Recovery Agent Rollout
 - Computers Requiring RS Agent Install
 - Computers Requiring RS Agent Upgrade
 - Computers with Local RS Agent Installed
 - Computers with Local-Only RS Agent Installed
 - Computers with RS Agent Installed
 - Computers with RS Agent Requiring Promotion
 - Computers with Server-Mode RS Agent Installed
 - Computers with Server-Only RS Agent Installed
 - Computers with Uninstalled RS Agent
 - RS Agent Enterprise Package
 - RS Agent Install
 - RS Agent Install in Local Mode
 - RS Agent Promotion
 - RS Agent Reinstall
 - RS Agent Uninstall
 - RS Agent Upgrade
 - Recovery Agent Settings
 - Recovery Solution Clusters - Licensing
 - Upgrade/Install Additional Solutions

The main content area is titled "RS Agent Install". It contains the following fields:

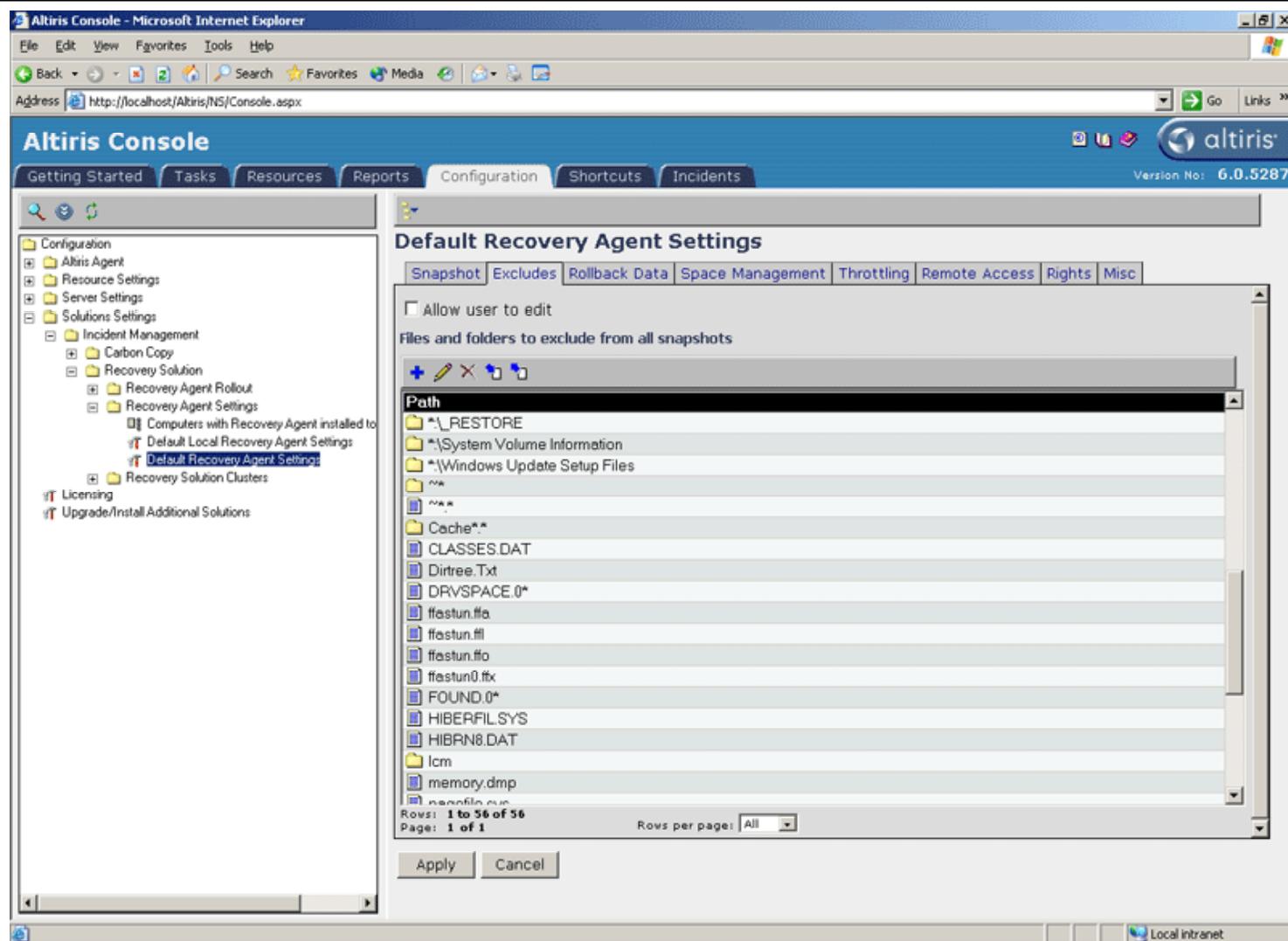
 - Enable (currently not enabled)
 - Name: RS Agent Install
 - Description: Install the Recovery Solution Agent.
 - Package name: RS Agent Enterprise Package
 - Program name: Install RS Agent
 - Enable status events
 - RS Cluster name: MYRS
 - Reboot computers automatically
 - Disable computers by default
 - Disable initial snapshot
 - Applies to collections: Computers Requiring RS Agent Install [Edit](#)

The "Scheduling Options" section includes:

 - Manual
 - Scheduled
 - Run once ASAP
 - Schedule: No schedule has been defined
 - Only run at scheduled time
 - Run as soon as possible after the scheduled time
 - User Can Run
 - Notify user when the task is available
 - Warn before running

At the bottom are "Apply" and "Cancel" buttons.

Altiris Patch Management Solution: Screenshot 2





TM

Tool: BMC Patch Manager

BMC Patch Manager enables you to manage and deploy security and functional patches on desktops, laptops, PDAs, and servers

By automating critical patch management functions (patch collection, preparation, testing, staging, deployment, auditing), it helps you to save time, improve response times, and reduce attack-related risks

Features:

- Provides patch-testing capabilities that allow administrators to group test patch installations within sample environments
- Allows you to deploy patches based on security policies for ongoing operations or specific tasks for emergency deployments
- Identifies vulnerabilities, automatically delivers critical patches, and fixes to thousands of endpoints, and verifies deployment success
- Allows you to proactively manage the distribution of patches including functional, anti-virus, and security patches to lower patch management costs



TM

BMC Patch Manager: Screenshot

The screenshot shows the BMC Configuration Management Report Center interface. The top navigation bar includes links for Applications, Common Tasks, Home, About, and Logout. Below the navigation is a menu bar with Queries, Query Library, and Policy Compliance selected. A status bar at the top right shows Status, Hide intro text, and Help.

The main content area is titled "Compliance Target View". It displays a message: "From this page you can see the subscription targets in your directory and the policy compliance associated for a target. <time zone information needed, console time vs. end-point time.>".

The left sidebar is a tree view of "Targets" under "Marimba > US". The "Engineering" node is expanded, showing its sub-nodes: Development, Finance, Field Services, HR, IT, Legal, Marketing, Office of CTO, Purchasing, Sales, Support, and Training. A search bar and a "Go" button are located above the tree.

The right panel is titled "Engineering" and shows "View compliance for: All policies affecting this target". It includes a "View Policy" button and options to "Show numbers" or "Show percentages". The overall compliance is shown as 70% (25% green, 45% red). The policy was last modified on 7/15/03 at 8:00AM, and 400 members were checked in out of 500. A table lists packages and their compliance status:

Package	Policy State	Compliance	Directly Assigned To
Emacs	Install	80% (20 green, 10 red, 10 blue)	Engineering
Internet Explorer 6.0	Install	70% (40 green, 20 red, 10 blue)	Mountain View
Trillian	Stage	100% (0 green, 0 red, 0 blue)	Mountain View
Visio	Advertise	100% (0 green, 0 red, 0 blue)	Engineering
WinZip	Install	90% (60 green, 5 red, 5 blue)	Mountain View

A legend at the bottom indicates: Green = Compliant, Red = Non-compliant, Blue = Not checked in.



TM

Tool: Hotfix Reporter

Hotfix Reporter is a tool that works in conjunction with the Microsoft Network Security Hotfix Checker (HfNetChk) tool to scan your network server for missing patches

HfNetChk scans your system for missing patches, but displays the results in a raw, plain-text, and unfriendly format

Hotfix Reporter converts the HfNetChk's raw output into an HTML page, complete with clickable links, making it easy to download the necessary patches from Microsoft

Features:

- Converts HfNetChk output into user-friendly HTML
- Tells you if the scan gave different results than the last time it was run, making it easy to quickly tell if any new patches have been released
- Displays Microsoft security bulletin numbers and knowledgebase article numbers as clickable links
- Shows the most recent patches first

Hotfix Reporter: Screenshot

Hotfix Reporter results - Microsoft Internet Explorer

Address: D:\Program Files\HfNetChk\results.htm

Hotfix Reporter < Reporter > Results from HfNetChk scan

Report generated: Wed Sep 03 08:50:52 2001.
Hotfix Reporter version 1.0 ([Check for updates!](#))

Notes:
See useful links at [bottom of report](#).
All links to external sites open into a new browser window.

Machine	Product	Bulletin	KB Q#	Patch status
MICRON	WINDOWS 2000 SP2	MS01-046	Q252795	NOT Found
The registry key ***SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q252795*** does not exist. It is required for this patch to be considered installed.				
MICRON	WINDOWS 2000 SP2	MS01-041	Q298012	NOT Found
File C:\WINNT\system32\catrv.dll has an invalid checksum and its file version is equal to or less than what is expected.				
MICRON	WINDOWS 2000 SP2	MS01-037	Q292755	NOT Found
The registry key ***SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q302755*** does not exist. It is required for this patch to be considered installed.				
MICRON	WINDOWS 2000 SP2	MS01-022	Q296441	WARNING
The XML file does not contain any file or registry details for this patch. As a result, this tool is unable to confirm that this patch has been applied. Please consider patch installation or refer to CYBERTRON for more information.				

My Computer



TM

Tool: Numara Patch Manager

Numara Patch Manager is a tool used to update and download patches for Microsoft's operating systems and applications across your entire network

It allows you to assess the patch status of all Microsoft-based workstations as well as validate any existing patches that have been installed

It creates baseline patch groups and scans groups of workstations to determine which ones are compliant and which ones are not

It can also be used to perform patch scans during non-business hours or off-peak bandwidth periods

Administrators can reboot workstations immediately or at a specified date or time

Numara Patch Manager: Screenshot

The screenshot displays the Numara Patch Manager application window. On the left, there is a sidebar with several sections:

- Scan What:** My Machine, My Domain, My Test Machines, Entire Network, New Machine Group...
- Favorites:** New Patch Favorite...
- Today's Items:** 4:09:58 PM (1)
- Patch Scanning:** QuickScan, FullScan, WUScan, New Patch Scan Template...
- Patch Groups:** New Patch Group...

The main area shows a grid of patch items with columns for Type, QNumber, Item, Deployment, Description, and Product. Many patches are marked as "Missing Service..." or "Patch Found". A detailed view of the "Acrobat Reader 7.0.8 Adobe Reader 7.0.8" patch is shown on the right, including its status, bulletin ID, item ID, summary, and download link.

Type	QNumber	Item	Deployment	Description	Product
Missing Service...				.NET Framework 2.0 SP1	.NET
Missing Service...				MSXML 3.0 SP7	MSXI
Missing Service...				Office 2003 SP3	Office
Missing Service...				Project 2003 Standard SP3	Proj
Missing Service...				SQL Server 2005 SP4	SQL
Missing Service...				SQL Server 2005 SP4	SQL
Missing Service...				SQL Server 2005 SP4	SQL
Missing Service...				SQL Server 2005 SP4	SQL
Missing Service...				SQL Server 2005 SP4	SQL
Missing Service...				SQL Server 2005 SP4	SQL
Missing Service...				WinZip 9.0 SP1	WinZ
Patch Found	QAR0708	AR70-008		Adobe Reader 7.0.8	Acrot
Patch Found	QFF2120	FF08-001		Mozilla Firefox Security Update	Firef
Patch Found	Q873339	MS04-043		Vulnerability in HyperTerminal Could Allo...	Wind
Patch Found	Q885835	MS04-044		Vulnerabilities in Windows Kernel and LS...	Wind
Patch Found	Q890175	MS05-001		Vulnerability in HTML Help Could Allow ...	Wind
Patch Found	Q886903	MS05-004		ASP.NET Path Validation Vulnerability [8...	.NET
Patch Found	Q888302	MS05-007		Vulnerability in Windows Could Allow Inf...	Wind
Patch Found	Q887472	MS05-009		Vulnerability in PNG Processing Could All...	Wind
Patch Found	Q885250	MS05-011		Vulnerability in Server Message Block C...	Wind



TM

Tool: TrueUpdate

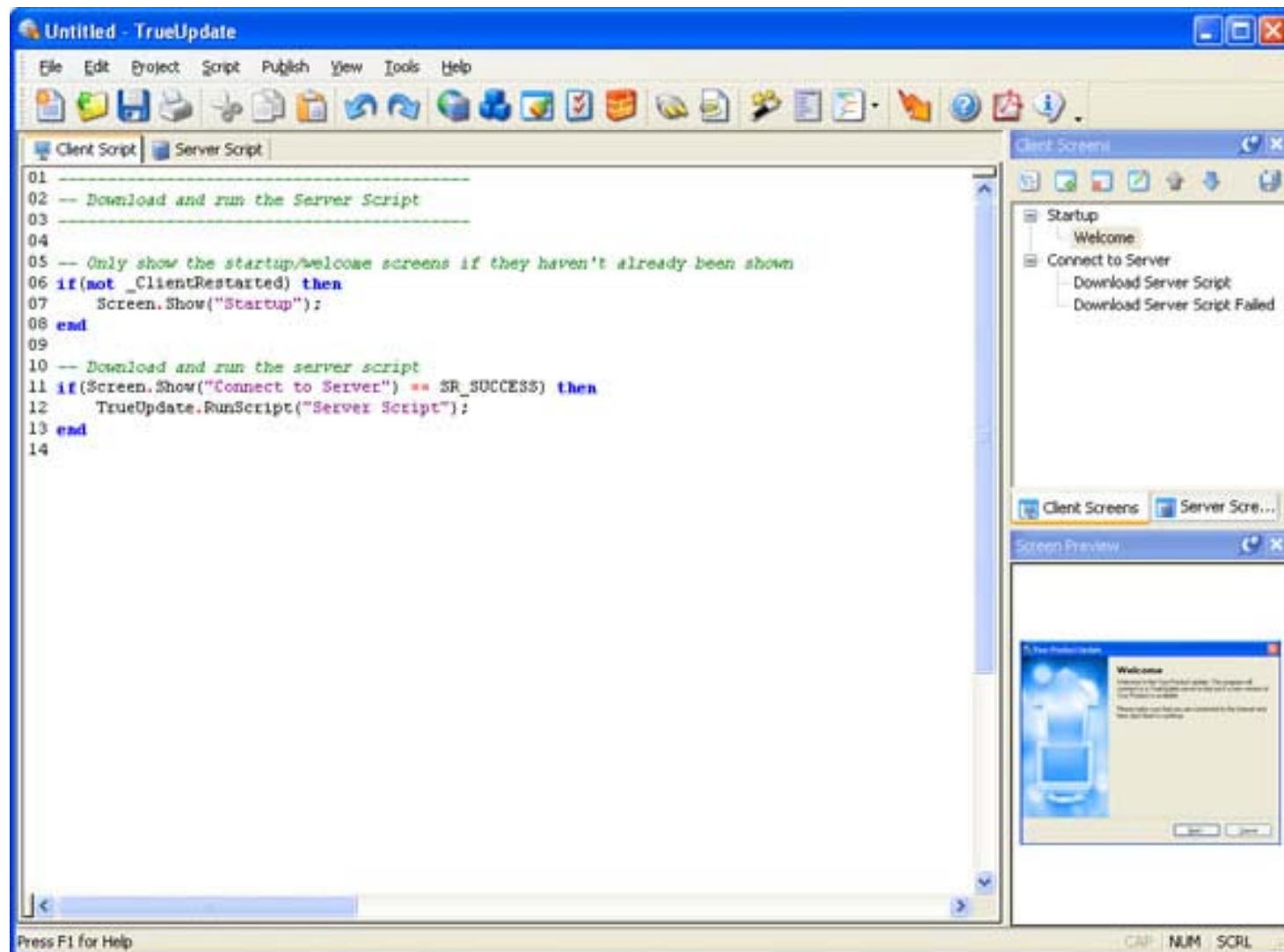
TrueUpdate is a comprehensive solution for software developers wanting to integrate automatic updating capabilities into their software applications

It gives you a robust client/server framework for determining required updates, and then retrieving and applying the necessary patches or installation files using standard Internet protocols

Features:

- The client can easily be integrated into existing software or installed as a standalone application
- Compatible with any update/patching method, from full setups and self-contained binary patches to download and extract from zip files
- The system is always up-to-date with the latest software and patches
- Includes more than 250 high level actions with everything from registry editing and file copying to web server script interaction and much more

TrueUpdate: Screenshot 1





TM

TrueUpdate: Screenshot 2

The screenshot shows the TrueUpdate application window. The main area is a code editor titled "tu30.tu2 - TrueUpdate" containing a Client Script. The script code is as follows:

```
01 --- Download and run the Server Script
02
03
04
05 -- Test mode - turned on by /TESTMODE command line argument.
06 -- This mode makes it try the i and i server first.
07 -- If running update tests, upload only to the i and i site
08 -- and pass the /TESTMODE cmd line arg.
09 g_IsTestMode = false;
10
11 local strArg = "";
12 local i = 0;
13 if(_CommandLineArgs)then
14     for i, strArg in _CommandLineArgs do
15         if(String.CompareNoCase(strArg,"/TESTMODE") == 0)then
16             g_IsTestMode = true;
17             Dialog.Message("Notice", "You are in test mode.");
18         end
19     end
20 end
21
22 -- Is it a quiet update (silent until update available)?
23 function IsQuietUpdate()
24     local bFound = false;
25     for i, arg in _CommandLineArgs do
26         if(arg == "/QUIET")then
27             bFound = true;
28         end
29     end
30     return bFound;
31 end
32
33 -- This will tell us:
34 g_IsQuietUpdate = IsQuietUpdate();
```

To the right of the code editor are two panes: "Client Screens" and "Screen Preview". The "Client Screens" pane shows a tree view of screens under the "Startup" category, including "Welcome", "Connect to Server", "Download Server Script", and "Download Server Script Failed". The "Screen Preview" pane is currently empty.



TrueUpdate: Screenshot 3

The screenshot shows the TrueUpdate application window titled "tu30.tu2 - TrueUpdate". The main area is a code editor with the following script content:

```
001
002 -- Server Script Configuration Variables
003
004
005
006 function ReadSerialFromSystem()
007     local strAppDataCommon = Shell.GetFolder(SHF_APPLICATIONDATA_CO
008     local strXMLFile = String.TrimRight(strAppDataCommon,"\\");
009     strXMLFile = strXMLFile.."\\IndigoRose\\TrueUpdate\\3.0\\trueup
010
011     if(File.DoesExist(strXMLFile))then
012         XML.Load(strXMLFile);
013         if(Application.GetLastError() == 0)then
014             local strSerial = XML.GetValue("CommonData/Serial");
015             if(strSerial ~= "")then
016                 return strSerial;
017             end
018         end
019     end
020
021     return "";
022 end
023
024
025 g_IRCustomerUpdatePHPscript = "http://www.indigorose.com/customers/
026
027 -- Get the Install Dir.
028 g_InstallDir = Registry.GetValue(HKEY_LOCAL_MACHINE, "Software\\Ind
029
030
031 -- Determine which product type is being used:
032 -- Written out to an INI file during install: cm or ev
033 g_ProductType = "cm"; -- Assume commercial
034 local strValue = INIFile.GetValue(g_InstallDir.."\\Data\\inf.ini","
035 &errValue = "err" then
```

The interface includes a toolbar at the top, a "Client Screens" panel on the right listing "Startup", "Welcome", "Connect to Server", "Download Server Script", and "Download Server Script Failed", and a "Screen Preview" window below it.



TM

Tool: FlashUpdate

FlashUpdate is a software update solution for windows developers

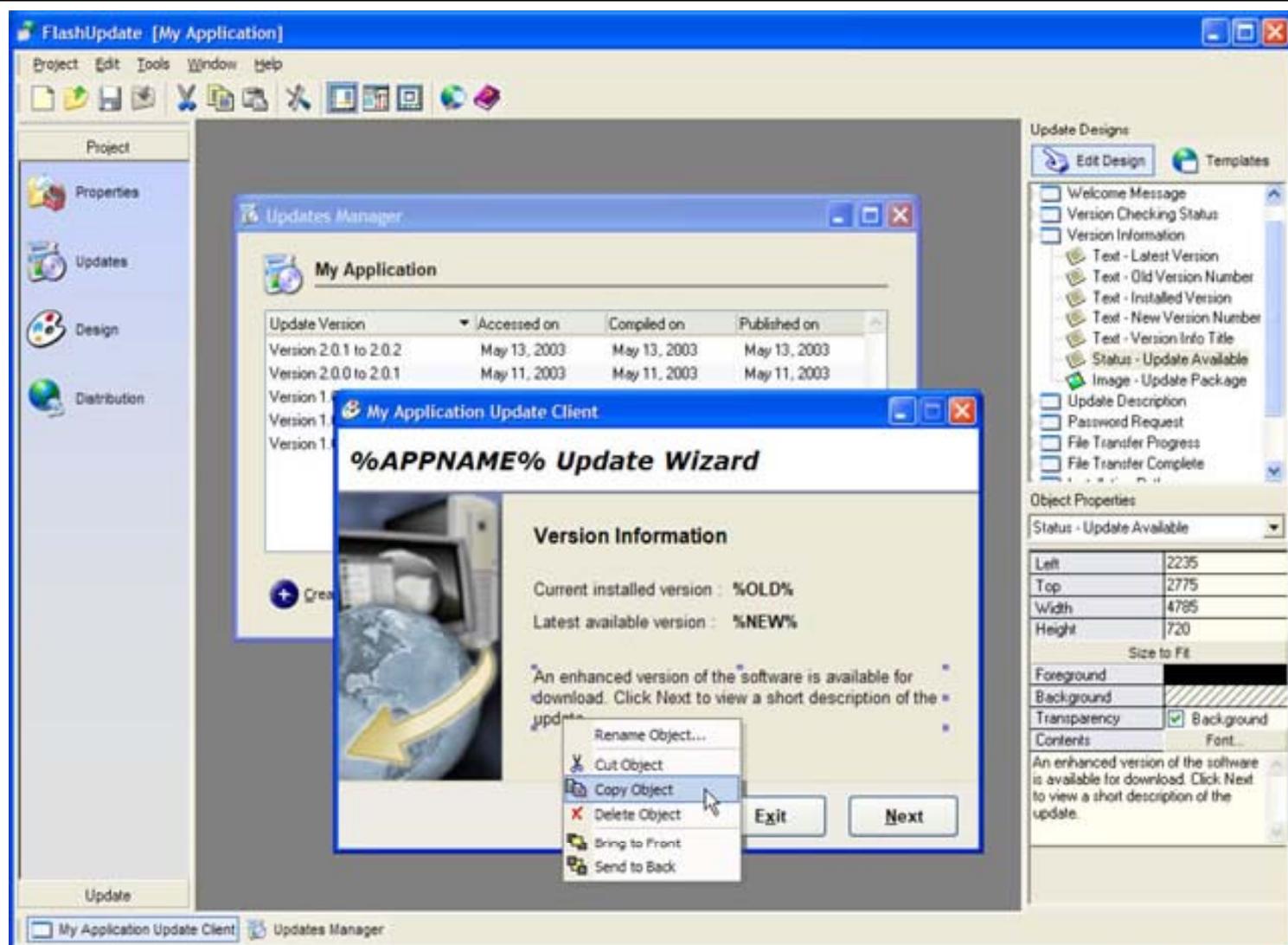
It allows you to create, manage, and distribute your software updates and patches in a flash

Features:

- Advanced Patch Engine provides up to 98% file compression
- Adaptive patch creation for optimal patch size and speed efficiency
- Support for all file types, including executable files, system files, data files, and documents
- Native support for shared and locked files
- Helps to prevent software piracy



FlashUpdate: Screenshot





TM

Tool: Microsoft Software Update Services (SUS)

Software Update Services (SUS) supports updating for a broader set of Microsoft products and provides robust management and reporting features

It connects through your firewall to the windows update site and allows IT administrators to import critical updates, security updates, and service packs

Administrators can receive e-mail notification when updates are added to their SUS pipeline

It consists of both client-side and server-side components to provide a basic solution to critical update management

Microsoft Software Update Services (SUS): Screenshot 1

The screenshot shows a Microsoft Internet Explorer window displaying the Microsoft Software Update Services (SUS) interface. The address bar shows the URL <http://w2ksrv1/susadmin/>. The page title is "Microsoft Software Update Services". The main content area displays a "Welcome" message and a "Welcome to Microsoft Software Update Services" section. On the left, there is a navigation pane with links like "Welcome", "Synchronize server", "Approve updates", "View synchronization log", "View approval log", "Set options", "Monitor server", "About Software Update Services", "Microsoft Windows Update", and "Microsoft Security". The bottom of the page includes copyright information for Microsoft Corporation and a link to the Local Intranet.

Microsoft Software Update Services (SUS): Screenshot 2

The screenshot shows a Microsoft Internet Explorer window displaying the Microsoft Software Update Services (SUS) interface. The address bar shows the URL <http://w2ksrv1/susadmin/>. The page title is "Microsoft Software Update Services". On the left, a sidebar menu lists options: Welcome, Synchronize server (which is selected), Approve updates, View synchronization log, View approval log, Set options, and Monitor server. Below this is a "See Also" section with links to About Software Update Services, Microsoft Windows Update, and Microsoft Security. The main content area is titled "Synchronize server" and displays information about the last synchronization (15:26:01 2003) and the next synchronization (None). It includes a "Synchronize Now" button and a "Synchronization Schedule" link. The bottom of the page includes standard copyright and footer links.



TM

Tool: Prism Patch Manager

Prism Patch Manager automatically secures windows systems from software vulnerabilities by managing the entire software patching process

It manages the software patching process such as discovering vulnerabilities, acquiring and testing patches, and deploying patches

It delivers comprehensive reporting to demonstrate patch compliance to management and auditors

It reduces organizational risk, improves IT productivity, and lowers the cost of IT infrastructure maintenance



Prism Patch Manager: Screenshot 1

The screenshot shows a Windows Internet Explorer window displaying the 'New Boundary Prism Patch Manager' application. The title bar reads 'New Boundary Prism Patch Manager - Windows Internet Explorer'. The address bar shows 'http://ppm'. The page header includes the Prism Patch Manager logo, the server date and time ('2/20/2008 10:33:25 AM (UTC-06:00)'), and links for 'About', 'Log Out', and 'Help'. The main menu bar has options like File, Edit, View, Favorites, Tools, and Help. Below the menu is a toolbar with icons for Home, Vulnerabilities, Deployments, Devices, Groups, Users, Reports, and Options. The 'Vulnerabilities' tab is selected. The main content area displays a table of vulnerabilities with columns for Impact, Status, and other metrics. The table lists various Microsoft patches and Adobe Acrobat Reader updates. At the bottom, there are navigation links for Deploy, Disable, Enable, Export, Update Cache, Scan Now, and a status bar indicating 'Local intranet' and '100%'.

Vulnerability Name	Impact	Critical	0	1	0	0	1	100%
MS07-028 931906 Vulnerability in CAPICOM (SEE NOTES)	Critical - 01	0	1	0	0	1	100%	
MS07-042 936227 936181 Vulnerability in Microsoft XML Core Services (MSXML4) (Rev 3)	Critical - 01	0	1	0	0	1	100%	
MS06-061 924191 925672 925673 Vulnerabilities in Microsoft XML Core Services (MSXML4)	Critical - 05	0	1	0	0	1	100%	
MS06-071 928088 927978 Vulnerability in Microsoft XML Core Services (MSXML4) (Rev 2)	Critical - 05	0	1	0	0	1	100%	
Scan Report for WMF Vulnerability (912840) Third Party Temporary Workaround wmfhotfix...	Critical - 05	0	1	0	0	1	100%	
MS 887606 Update for MSXML 2.0 SP6	Recommended	0	1	0	0	1	100%	
MS 887606 Update for MSXML 4.0 SP2	Recommended	0	1	0	0	1	100%	
MS 909520 Microsoft Base Smart Card Cryptographic Service Provider Package	Recommended	0	1	0	0	1	100%	
MS 909915 Patch 1 for installing Australian Daylight Saving time zones for year 2006 (SE...	Recommended	0	1	0	0	1	100%	
MS 932590 DST update to C Runtime Library msvcrtd.dll for C applications	Recommended	0	1	0	0	1	100%	
MS 941833 Update for Microsoft XML Core Services 4.0 Service Pack 2	Recommended	0	1	0	0	1	100%	
Adobe Acrobat Reader 6.0	Software	0	1	0	0	1	100%	
Adobe Acrobat Reader 6.0.1	Software	0	1	0	0	1	100%	
Adobe Acrobat Reader 7.0.5	Software	0	1	0	0	1	100%	
Adobe Acrobat Reader 7.0.7	Software	0	1	0	0	1	100%	



TM

Prism Patch Manager: Screenshot 2

The screenshot shows the 'Configuration' tab of the Prism Patch Manager web interface. The page title is 'New Boundary Prism Patch Manager - Internet Explorer'. The URL is http://wilbur/default.aspx?page=admin2. The top menu includes File, Edit, View, Favorites, Tools, and Help. The toolbar includes Back, Forward, Stop, Refresh, Home, Page, Tools, and a search bar for Google.

The main header features the 'PRISM PATCH MANAGER' logo and navigation links for Home, Vulnerabilities, Deployments, Devices, Groups, Users, Reports, and Options. The 'Options' link is highlighted in red. The server date and time are displayed as 3/12/2008 2:25:29 PM (UTC-05:00). The top right corner has links for About, Log Out, and Help.

The configuration page is divided into sections:

- Deployment Defaults**: Set your deployment defaults.
 - Concurrent**: Maximum number of Deployments that can run simultaneously (Deployment Limit)
 - Maximum number of Discover Applicable Update System tasks that can be run simultaneously (DAU)
 - Maximum number of Reboot tasks that can be run simultaneously
 - Maximum number of Simultaneous mandatory baseline deployments
- Consecutive**: Maximum number of times a deployment will be consecutively attempted
- Agent Defaults**: Set your Agent defaults.
 - Communication**: Agents should be shown Offline when inactive for Hour(s) Set to 0 (zero) to disable
 - Agent Uniqueness Based On:
- Notification Defaults**:
 - User Notification window should always be on top
 - Manual Installation (Max 256 Chars):**
This package will be downloaded
and made available for your
administrator to install.
171 characters left.
 - Default Deployment Message (Max 256 Chars):**
The download and installation of
the patch: {Package Name} is ready
to begin. If you require any
87 characters left.

At the bottom, there is a user profile for 'eric', and buttons for Save and Export. The status bar at the bottom indicates 'Local intranet | Protected Mode: Off' and '100%'. A copyright notice is visible at the bottom right: 'Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.'



TM

Tool: Patch-Magic

Patch-Magic updates all computer systems in your network

It avoids viruses and worms, and minimizes security risks

It can be used to scan each system individually, to discover necessary patches and updates, and to install them remotely

Features:

- Intuitive view and description of missing patches
- Automates patch download and individual deployment
- Identifies and removes remote malware in your LAN
- Time scheduler for scans, deployment, and data base update
- Supports virus scanning proxy servers / firewalls
- Centralized storage of patches at the location of your choice (patch library)
- Intelligent reboot handling



TM

Patch-Magic: Screenshot

The screenshot shows the VisLogic Patch-Magic V3.0 application window. The left sidebar contains a navigation tree with the following structure:

- Patch-Magic Systemmenü
 - Netzwerk Übersicht
 - Computer sortiert
 - Vollständig up to date
 - Updates ausstehend
 - Reboot ausstehend
 - Malwareverseucht
 - Problemrechner
 - Unlizenzierte
 - Funktionen per Doppelklick
 - PCs manuell hinzufügen
 - Pool löschen
 - Ereignisprotokoll
 - Patchdatenbank
 - Einstellungen
 - Zeitplan
 - Anti Malware Einstellungen
 - Netzwerkeinstellungen
 - Sonstige Einstellungen
 - Spracheinstellungen
 - VisLogic Onlinedienste
 - Sonstiges

Microsoft Windows-Netzwerk (9 von 50 lizenzierten Nodes)

- IP-Range
- Scanprobleme
- Scan-Pool
 - VISLOGIC, Microsoft Windows 2000, Deutsch
 - VISLOGIC2, Microsoft Windows 2000, Deutsch
 - Malware Scanergebnisse
 - Status.....Keine Infektion gefunden.
 - Letzter Scan...2008/03/17 12:17:24
 - Wichtige Updates
 - Bereits installierte
 - Knowledge Base Article 891861 (KB891861) : Update-Rollup 1 für Windows 2000 SP4
 - Windows 2000 Service Pack 4 (Q327194) : Windows 2000 Service Pack 4
 - Knowledge Base Article 828026 (KB828026) : Wichtiges Update für Skriptbefehle von Windows Media PI
 - Knowledge Base Article 893803 (KB893803) : Microsoft Windows Installer 3.1 (V2)
 - Knowledge Base Article 922582 (KB922582) : Fehlermeldung beim Versuch, MS Windows zu aktualisieren
 - Knowledge Base Article 927891 (KB927891) : Update für Windows 2000
 - MS02-050 (Q329115) : Sicherheitsanfälligkeit in Zertifikatsprüfung ermöglicht vorgetäuschte Identität
 - MS03-011 (KB816093) : Fehler in Microsoft VM kann eine Systemgefährdung ermöglichen

PC Name	Platform	Gruppe	Status
VISLOGIC	Microsoft Windows 2000	IP-Range	ready.
VISLOGIC1	Microsoft Windows XP	IP-Range	ready.
VISLOGIC2	Microsoft Windows 2000	IP-Range	ready.
VISLOGIC3	Microsoft Windows XP	IP-Range	ready.
VISLOGIC4		IP-Range	ready.
VISLOGIC5		IP-Range	ready.
VISLOGIC_TEST1		IP-Range	ready.
VISLOGIC_TEST2	kein Admin / Scantimeout / Firewall	IP-Range	Scanprobleme
VISLOGIC_TEST3	Microsoft Windows XP	IP-Range	ready.

www.patch-magic.com

Patch Management Checklist

How often and when do you apply patches?

Who can deploy and/or authorize updates?

How are patches tested prior to rollout?

What problems will trigger a rollback?





Best Practices for Patch Management

Test the patch before rollout to ensure that the applied patch is compatible with other applications

You need to have a rollback version when the applied patch fails

Do not deploy multiple patches simultaneously across the network as it will halt other applications and will be inconvenient for users

Deploy the patches after production hours as reboot is required for maximum patches

Always check for latest releases to minimize downtime as often a user calls or virus initiates a frantic search for a missing patch

If you patch regularly, you need to keep track of what fixes were applied, when, for auditing and reporting

Follow the defined patch process which specifies who may approve patches and procedures to deploy them



Summary

A hotfix is a code that fixes a bug in a product

Patch Management is the process of correcting deficiencies and updating software with the latest features

Windows patch management involves: testing, deployment, and validation

Microsoft Software Update Services (SUS) hosts windows updates

Designing a deployment plan to distribute patch on a timely basis is one of the best practices in the patch management