



Ethical Hacking and Countermeasures

Version 6



Module LXV

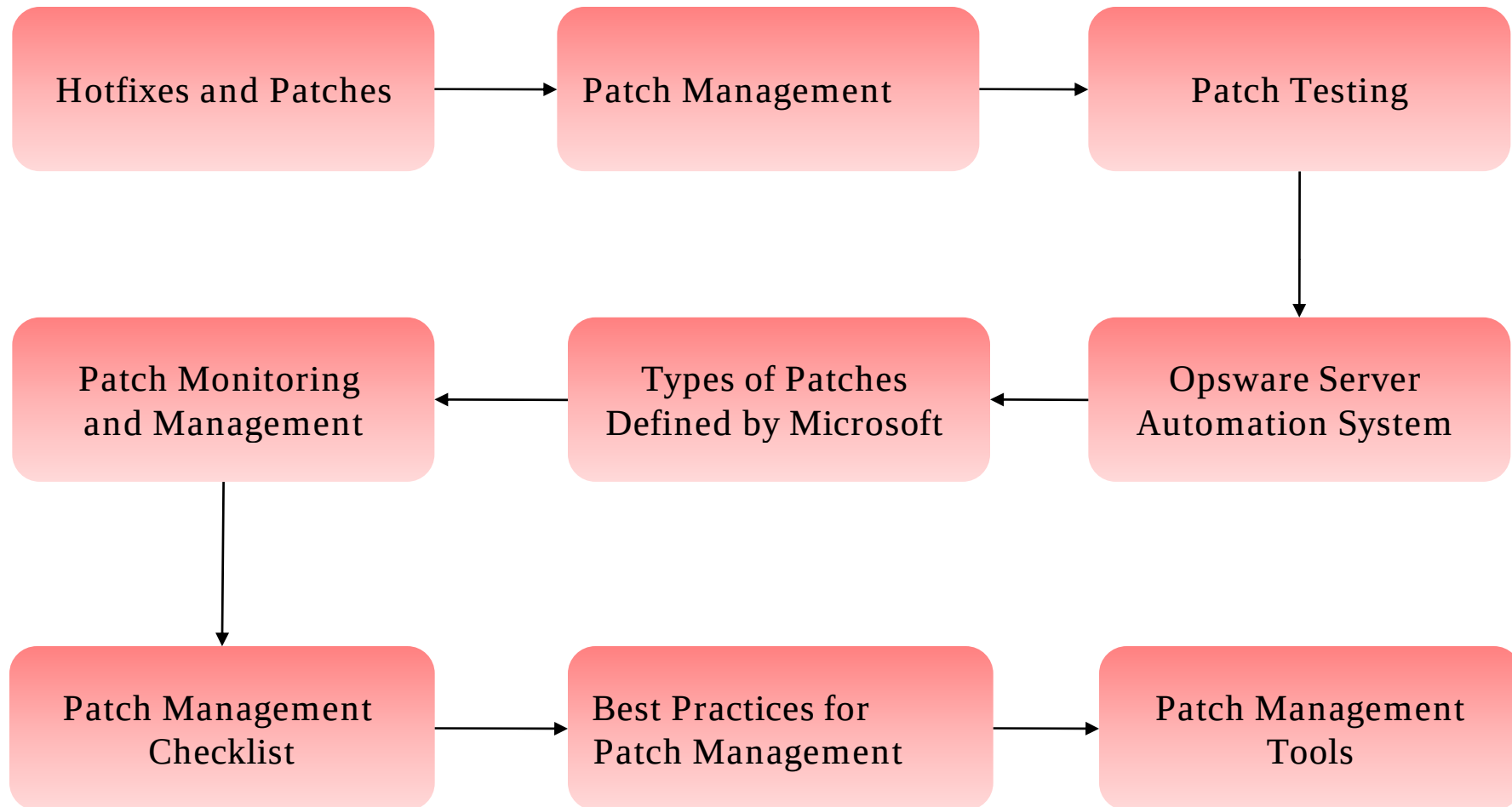
Patch Management

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
- Opware Server Automation System (SAS)
- Patch Management Checklist
- Best Practices for Patch Management
- Patch Management Tools

Module Flow



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

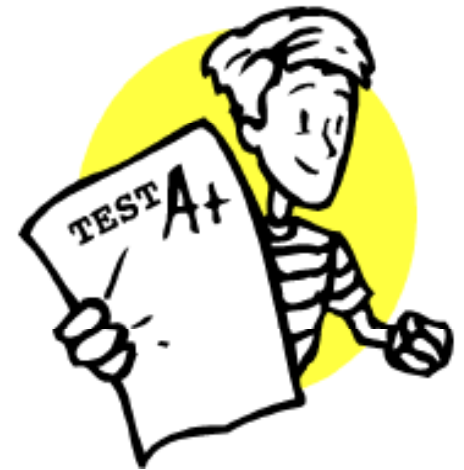
The first step in patch testing is the verification of patch source and integrity which helps you to ensure that update is valid and it is not altered

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

Opsware Server Automation System (SAS)

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

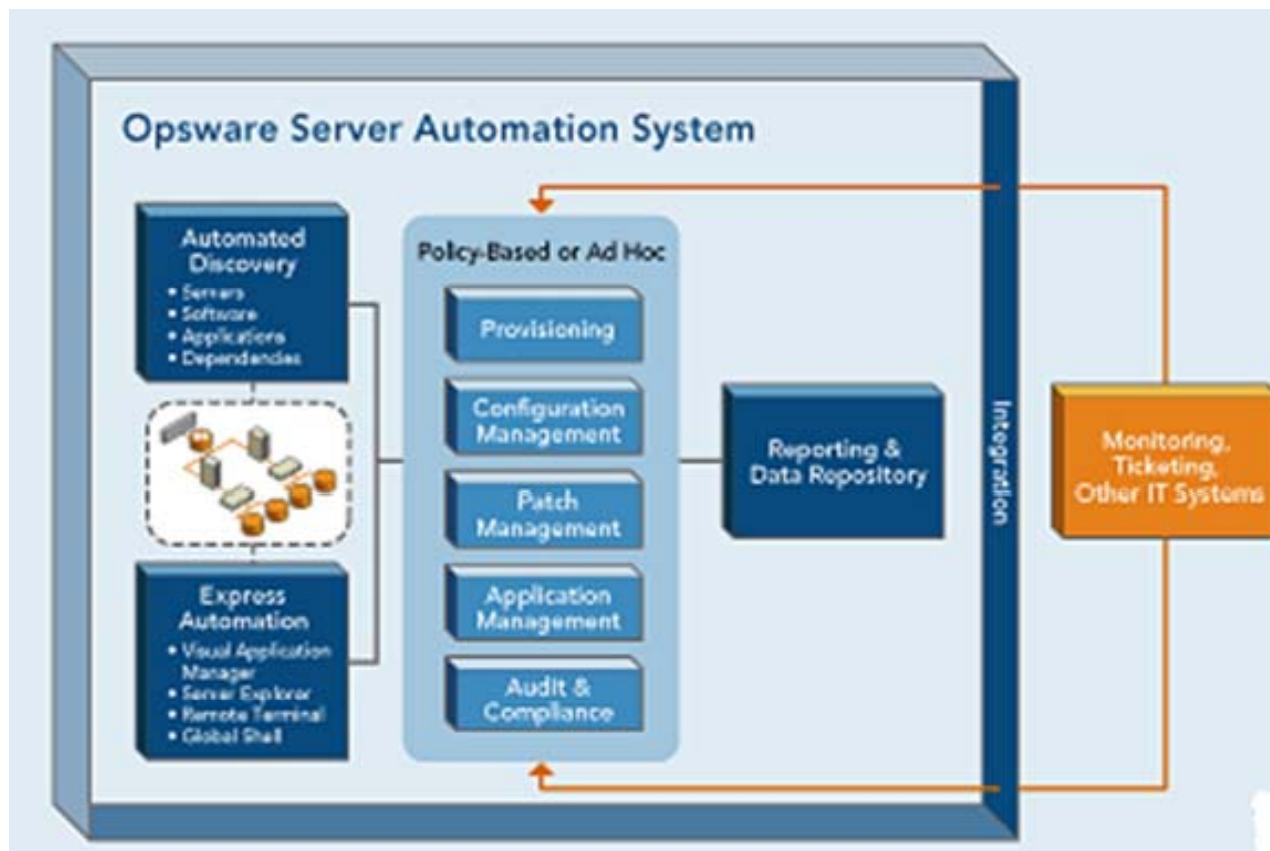
It gives administrators the ability to monitor systems and apply configuration changes across many servers in a uniform fashion

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

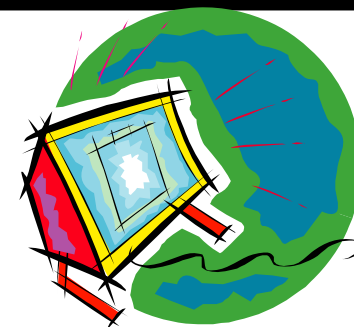
Opsware Server Automation System (SAS) (cont'd)



Patch Management Tools

Tool: UpdateExpert

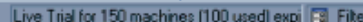
UpdateExpert is a Windows administration program that helps you to secure your systems by remotely managing service packs and hotfixes



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

Certified Ethical Hacker



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:\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
```

caccls.exe Utility

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

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

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



```
Command Prompt

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

C:\Snort>
```

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

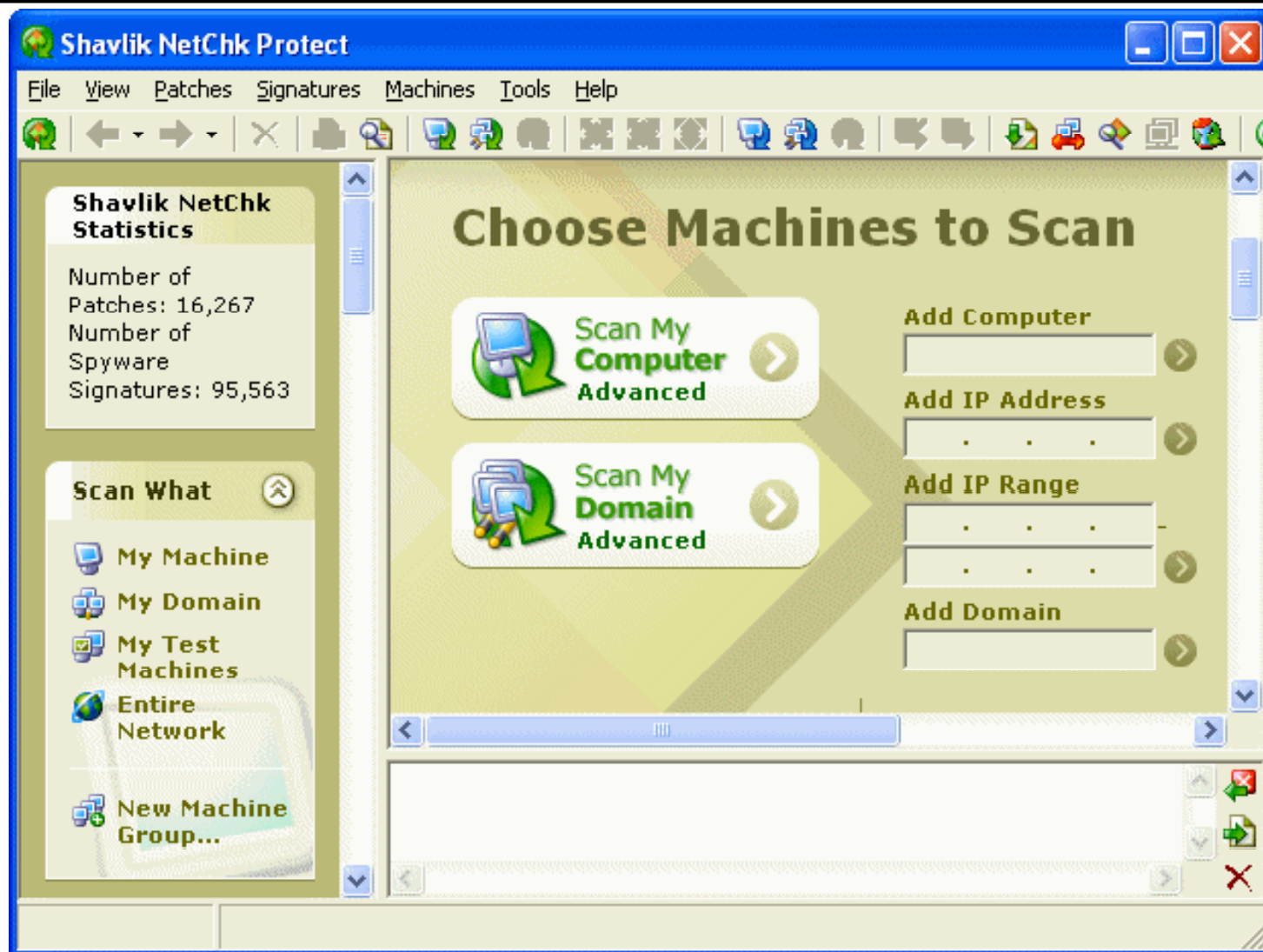
It offers a solution for detecting, removing, and managing critical threats and vulnerabilities with active vulnerability management

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

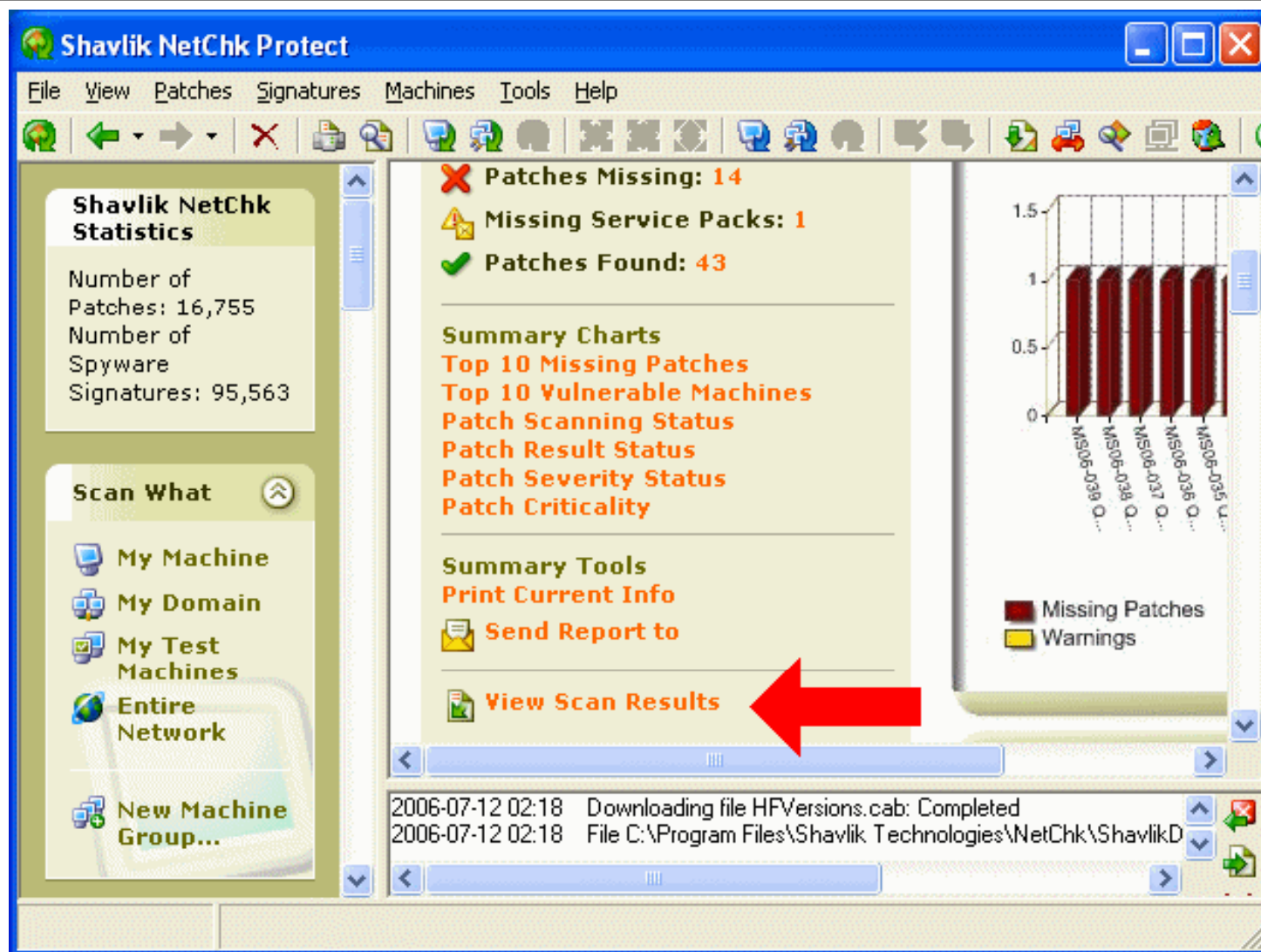
Features:

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

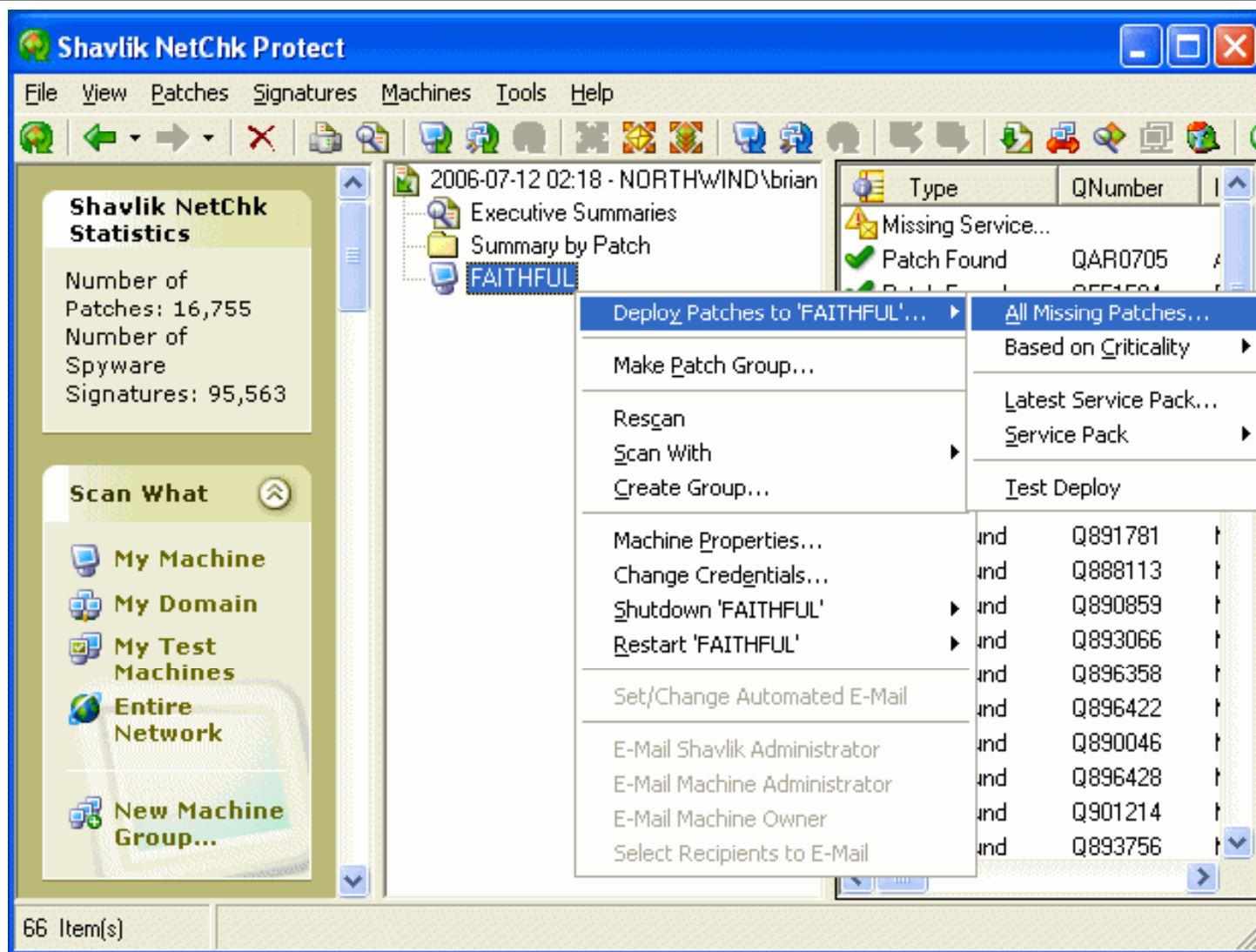
Shavlik NetChk Protect: Screenshot 1



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

Home Audit Scripts Monitor Ticketing **Patch Mgmt** Remote Cntl Backup Reports Agent System Log Off: Nick

Notes Status Machine ID Rows Select Machine Group Select View Reset

Help << < Select Page > >> 100 smc.smc < No View > Edit...

Function List

- Setup
 - Scan Machine
 - Patch Status
 - 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

Automatically apply all new patches and updates at the scheduled time of day.

Set Auto Every day at 3 am :00 Stagger by 5 min. Cancel

☒ Skip if machine offline

Select All ☒ Skip if machine offline
Unselect All Machine.Group ID Auto update time

ok	☐	KServer	
ok	☐	kcheck01.smc.smc	
ok	☐	kcheck02.smc.smc	

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

Kaseya Patch Management: Screenshot 2

Home Audit Scripts Monitor Ticketing **Patch Mgmt** Remote Cntl Backup Reports Agent System Log Off: Nick

Notes Status Machine ID Rows Select Machine Group Select View Reset

Help << < Select Page > >> 100 smc.smc < No View > Edit...

Function List

- Setup
 - Scan Machine
 - Patch Status**
 - 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

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

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.

[Select All](#) [Unselect All](#)

		Machine.Group ID	Installed Patches	Missing Approved	Missing Denied	Pending Logged In	User Not 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

Home Audit Scripts Monitor Ticketing **Patch Mgmt** Remote Cntl Backup Reports Agent System Log Off: Nick

Notes Status Machine ID Rows Select Machine Group Select View Reset

Help << < Select Page > >> 100 smc.smc < No View > Edit...

Function List

- Setup**
 - Scan Machine
 - Patch Status
 - 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

Apply Specify how to reboot after applying new patches and updates.

☐ Reboot immediately after update.
☐ Reboot every day at 12 am :00 after install.
☐ Warn user that machine will reboot in 5 minutes (without asking permission).
☐ Skip reboot if user logged in.
☐ If user logged in ask to reboot every 5 minutes until the reboot occurs. Reboot if user not logged in.
☒ If user logged in ask permission. Reboot if no response in 5 minutes. Reboot if user not logged in.
☐ If user logged in ask permission. Do nothing if no response in 5 minutes. Reboot if user not logged in.
☐ Do not reboot after update. ☐ Email when reboot required.

[Select All](#) [Unselect All](#)

	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

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

Tool: IBM Tivoli Configuration Manager

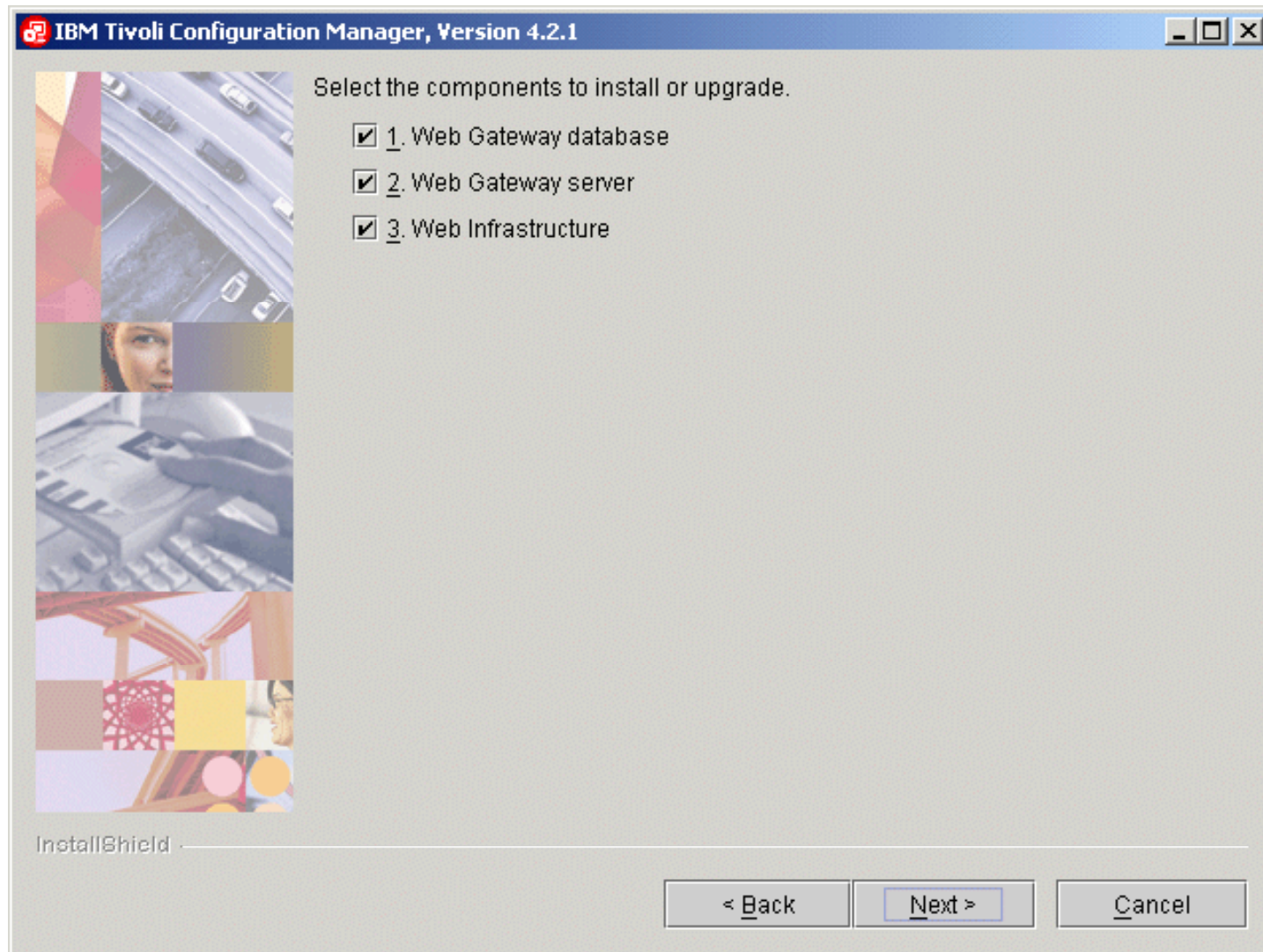
IBM's configuration manager provides Microsoft client and server software patch automation capabilities in distributed environments

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

IBM Tivoli Configuration Manager, Version 4.2.1

A Tivoli endpoint is not installed on your machine. Specify the endpoint configuration options on this screen. In the Endpoint options field, specify additional lcmd command options, as documented in the Tivoli Management Framework Reference Manual.

Destination directory

Gateway port

Endpoint port

Endpoint options

InstallShield

Tool: LANDesk Patch Manager

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

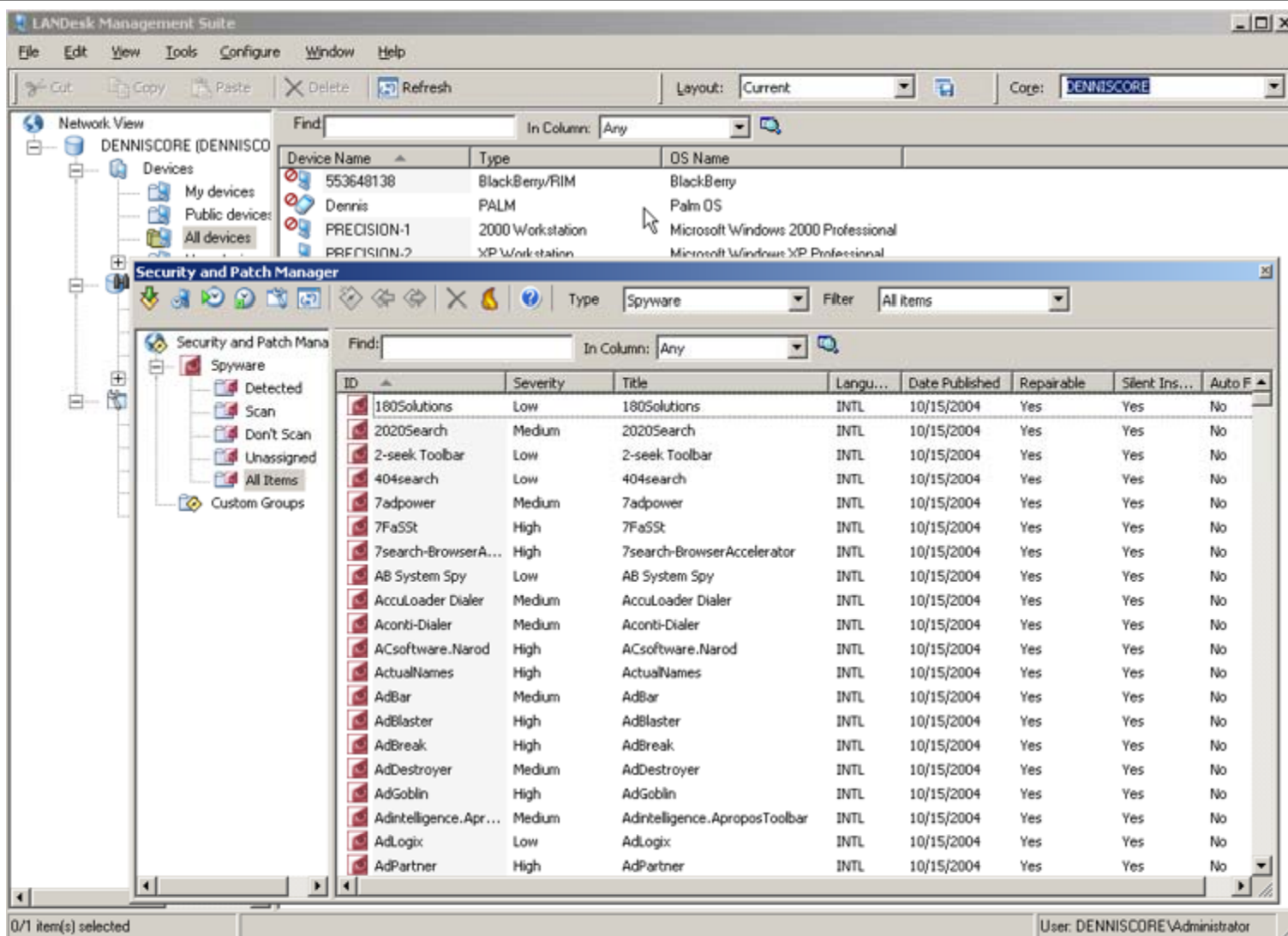
It scans managed devices to identify application and operating system vulnerabilities

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

LANDesk Patch Manager: Screenshot



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

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

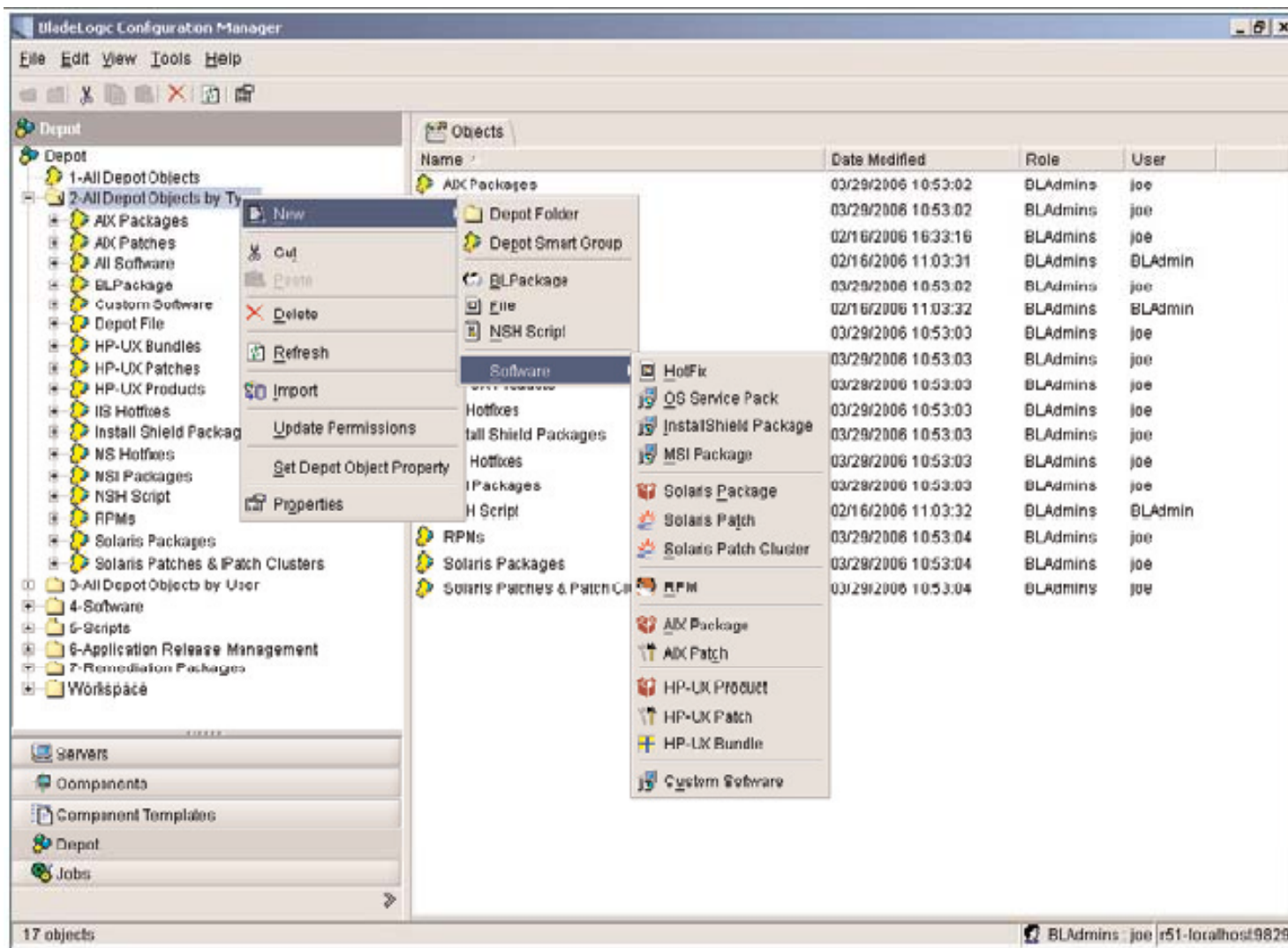
It features a cross-platform command line interface that supports a single-sign on using a range of authentication protocols

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

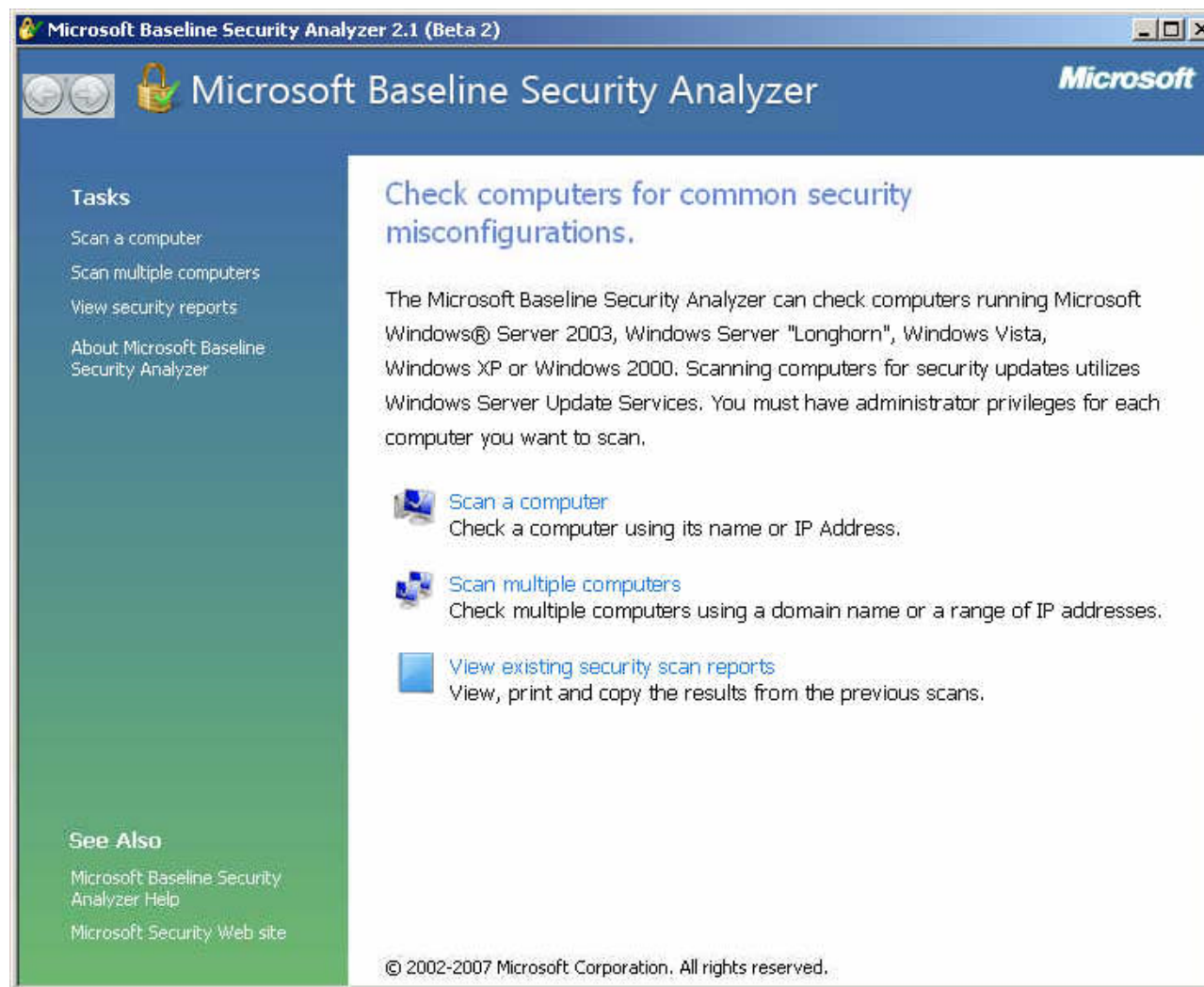
It scans and reports on updates designated as critical security updates by the Windows Update site

Procedure:

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



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] [-?]
```

Tool: QChain

Qchain allows to install multiple security updates

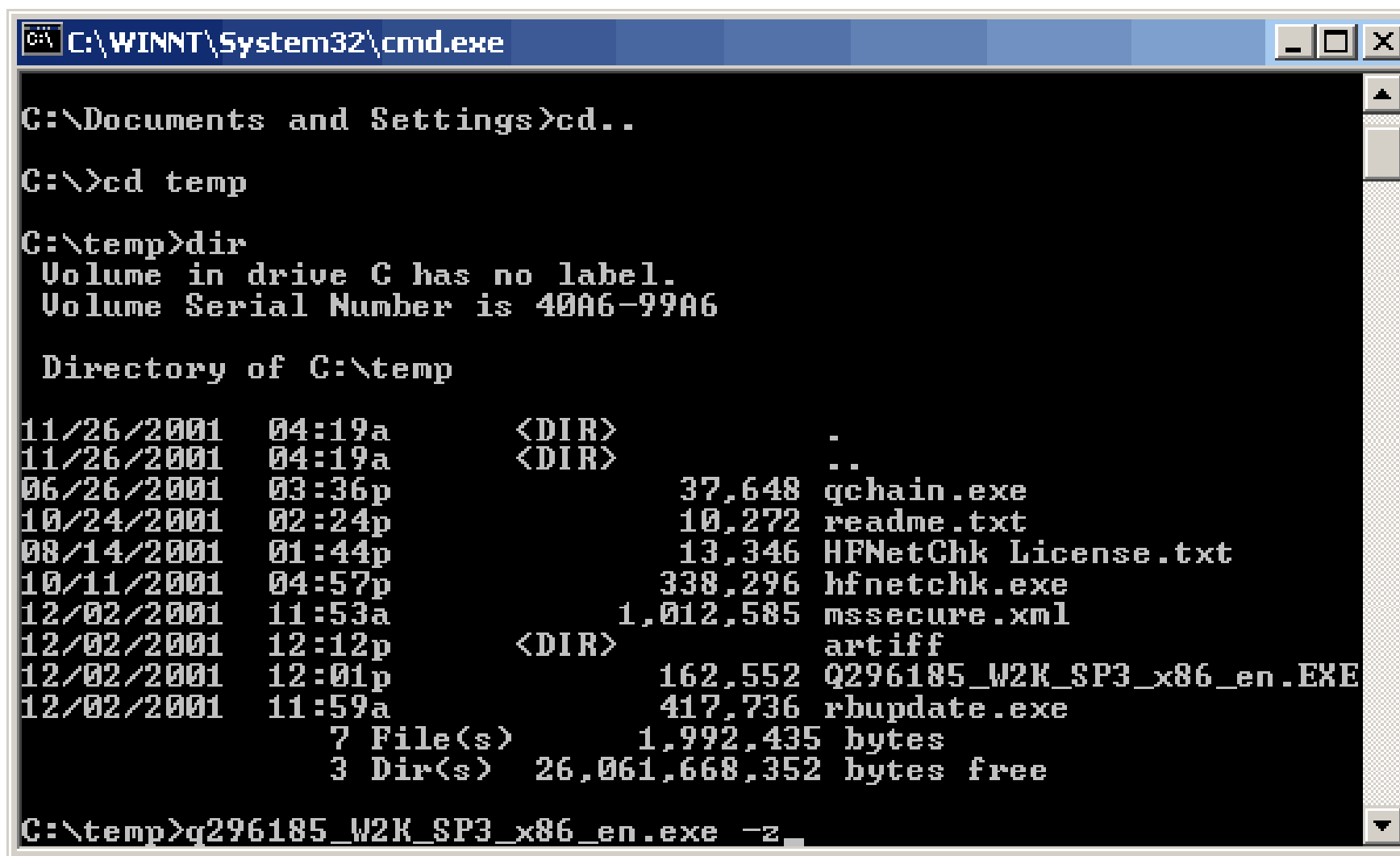
It evaluates the drivers, DLLs, and executable files updated by each security update

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



A screenshot of a Windows command prompt window titled "C:\WINNT\System32\cmd.exe". The window shows the following commands and output:

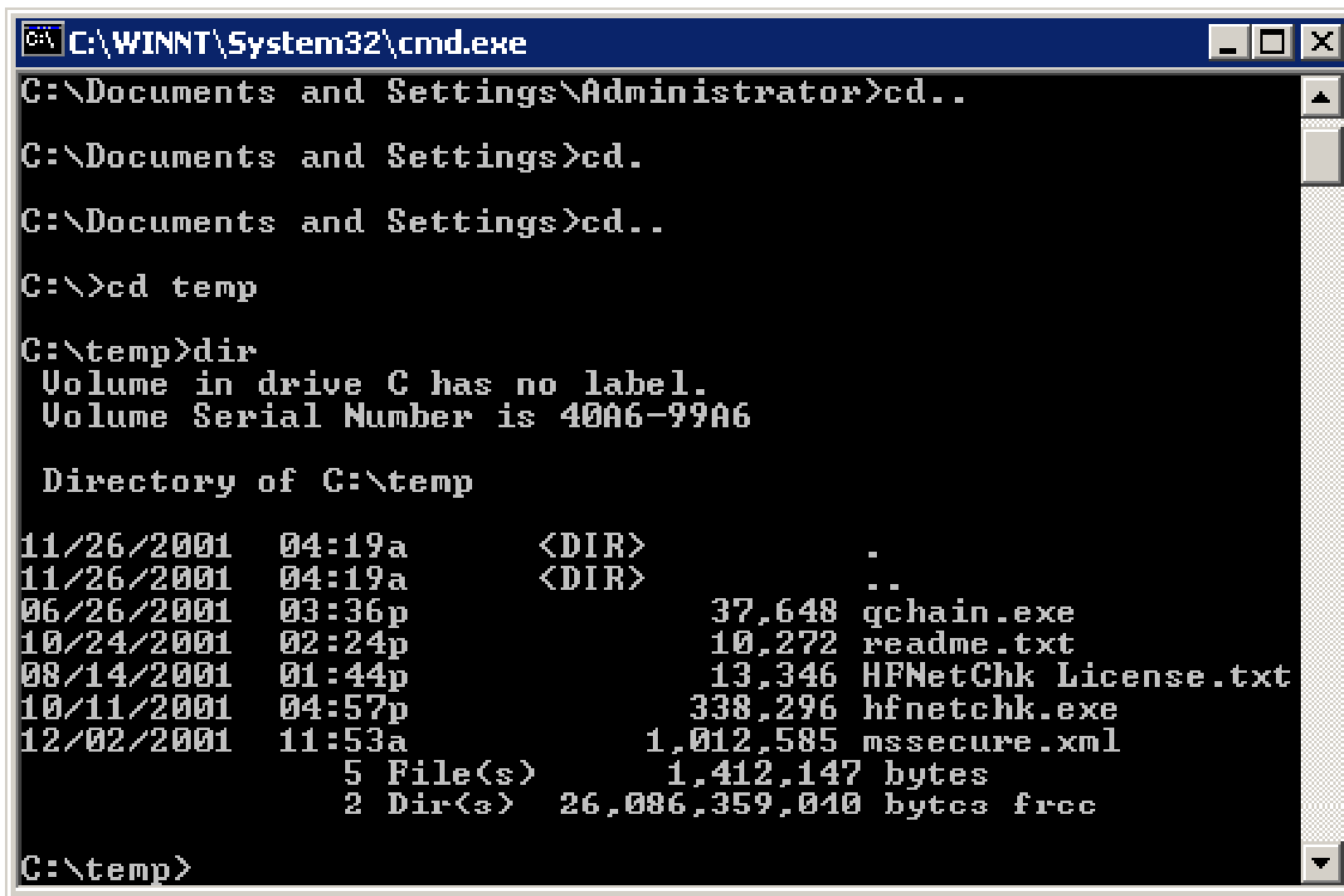
```
C:\Documents and Settings>cd..
C:\>cd temp
C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is 40A6-99A6

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_
```

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

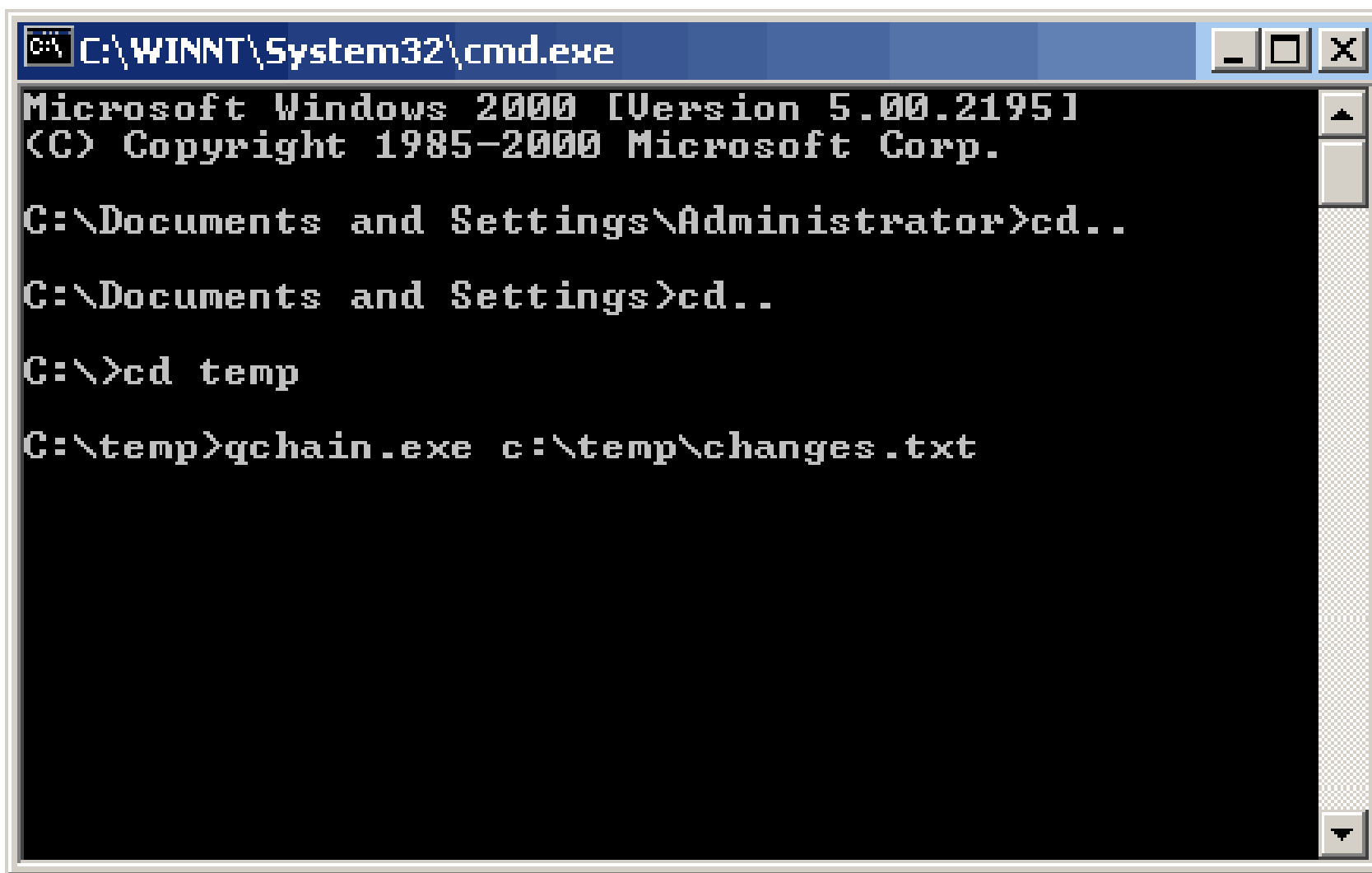
C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is 40A6-99A6

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)  26,086,359,040 bytes free

C:\temp>
```

Qchain: Screenshot 3



A screenshot of a Windows 2000 command prompt window. The title bar reads "C:\WINNT\System32\cmd.exe". The window contains 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 trail of every action and step taken on each computer during the patch management process

BigFix Enterprise Suite (BFS): Screenshot 1

The screenshot displays the BigFix Enterprise Console interface. The top window shows a list of vulnerabilities under the heading "All Relevant Fidet Messages (49)". The list includes several entries, with MS06-014 being highlighted. Below this, a detailed view of MS06-014 is shown, including a description of the vulnerability, its severity (Critical), and relevant computers (0). The detailed view also includes a section for "Patch Management Patches for Windows" and a description of the vulnerability.

Name	Source Sev...	Site
MS06-015: Vulnerability in Windows Explorer Could Allow Remote Code Execution - Windows XP SP1/SP2	Critical	Enterprise Sec.
MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - Windows XP(2003 (x64) - BE...	Critical	Enterprise Sec.
MS06-013: Cumulative Security Update for Internet Explorer - IE 6.0 - Windows XP SP2	Critical	Enterprise Sec.
MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - Windows XP SP1/SP2	Critical	Enterprise Sec.
MS06-013: Cumulative Security Update for Internet Explorer - IE 6.0 - Windows XP(2003 (x64) - BES < 6.0	Critical	Enterprise Sec.
MS06-005: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Pl...	Critical	Enterprise Sec.
MS06-015: Vulnerability in Windows Explorer Could Allow Remote Code Execution - Windows XP(2003 (x6...	Critical	Enterprise Sec.

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

0 Relevant Computers
0 Open Actions

Patch Management Patches for Windows

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

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.

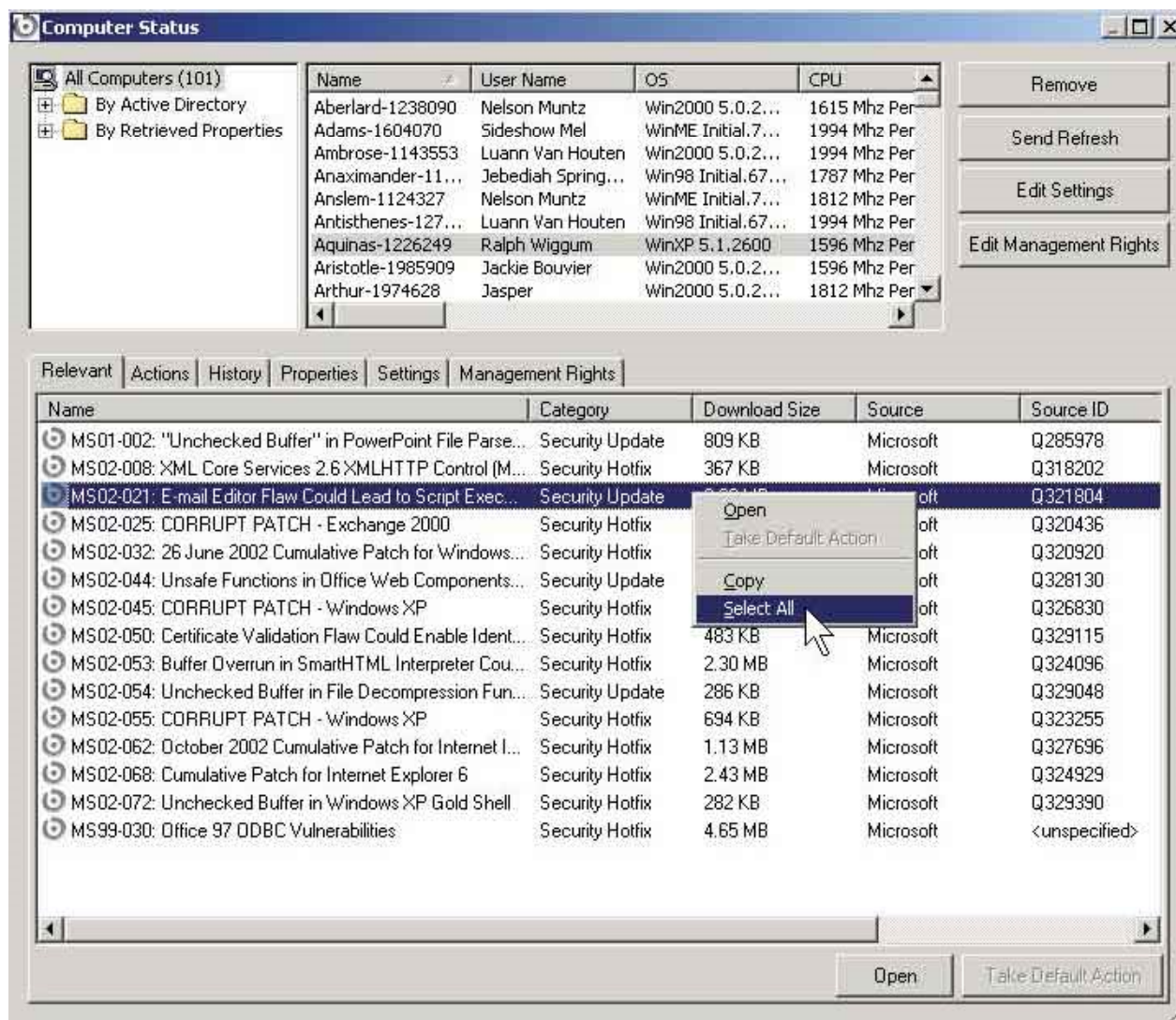
After downloading and installing this patch, affected computers will no longer be susceptible to these vulnerabilities.

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.

Ready | Connected to database "bfenterprise" as user "EvaluationUser" | N/A

BigFix Enterprise Suite (BFS): Screenshot 2



Tool: Shavlik NetChk Protect

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

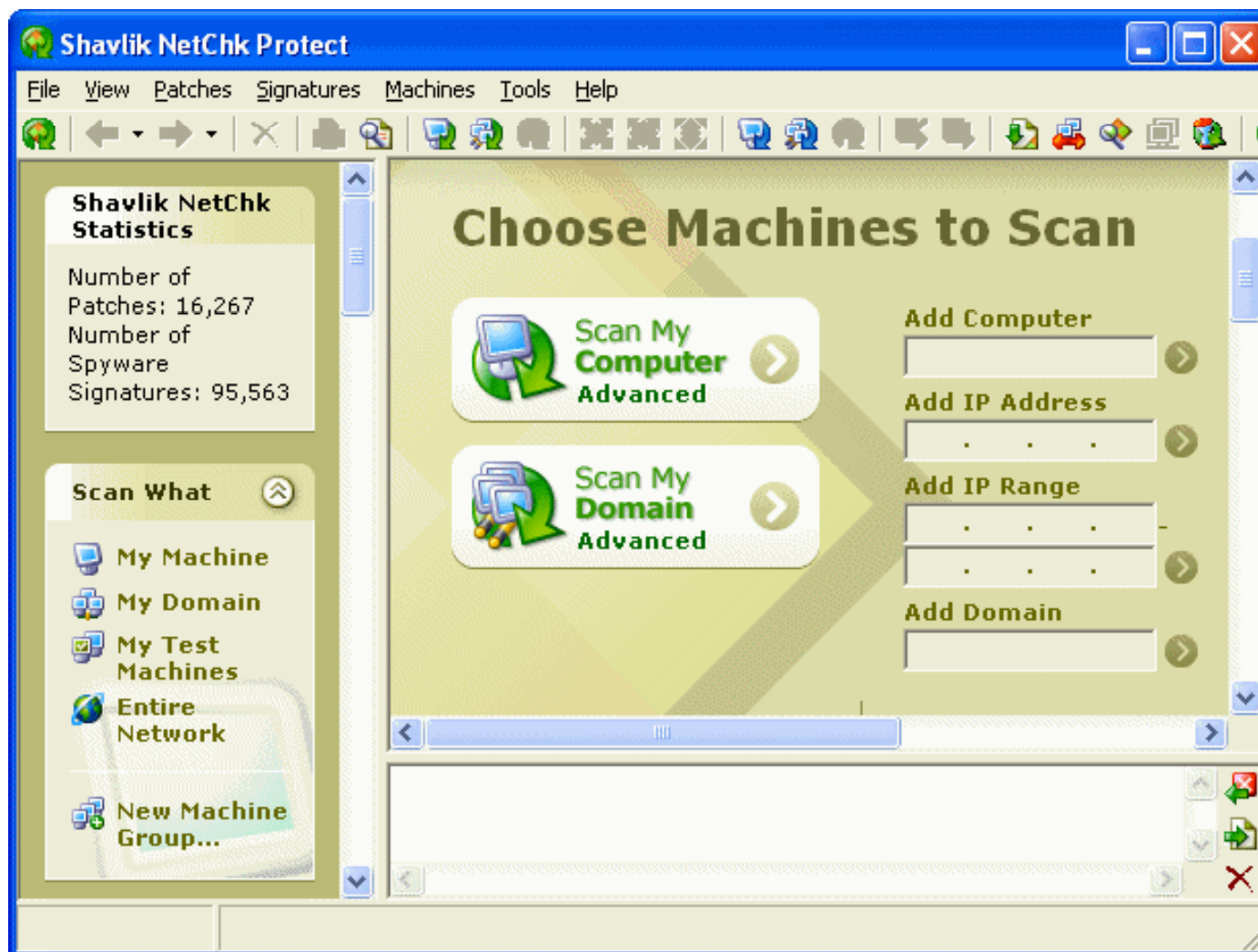
Features:

- 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



Tool: PatchLink Update

PatchLink Update is a patch and vulnerability solution for large networks

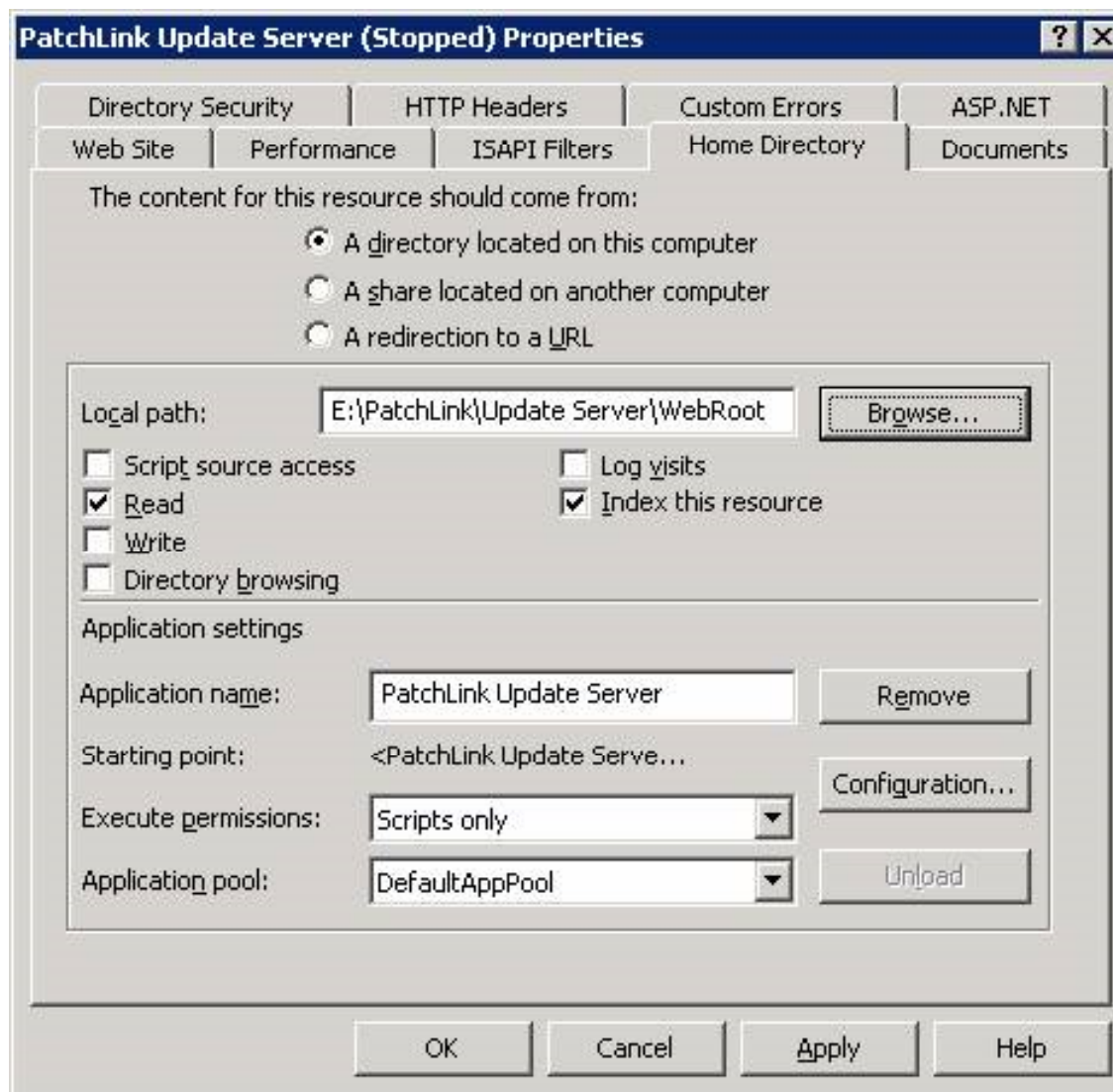
It scans networks for security holes using fingerprint technology

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



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

SecureCentral PatchQuest: Screenshot 1

secure | centralTM
PatchQuest

Feedback | About | Personalize | Help | License | Logout (admin)

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

Agent update!
Agent version is up-to-date.

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_updat...

Scan Result » sd-test3
Export Print Help

All Updates Security Updates Non-Security Updates Service Packs

Product Summary

Product Name	Service Packs	Available Patches	Missing Patches	Informational Items	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 SP2	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	5	3	0	0	0
Outlook 2000 Gold	5	0	0	0	0
Outlook Express 6.0 Gold	2	0	0	0	1
PowerPoint 2000 Gold	5	0	0	0	0
SQL Server 2000 Gold	5	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

Deploy Download Undeploy Add To Patch Group Search None like Go

Showing 1 to 25 of 8 Entries per page 25 Edit Column

Patch Status	Bulletin ID	Patch Name	Installation Status	Download Status	Severity
✓	MSRT-001	New Windows-KB890830-ENU.exe	NA	✓	✓
✓	MS99-044	z19v2ukw.exe	NA	✓	✓
✓	MS99-030	JetcoPkg.exe	NA	✓	✓
✓	MS06-078	New WindowsMedia6-KB925398-x86-ENU...	NA	✓	✓
✓	MS06-077	New Windows2000-KB926121-x86-ENU.E...	NA	✓	✓
✗	MS06-071	msxml4-KB927978-enu.exe	NA	✓	✗
✗	MS06-071	msxml6-KB927977-enu-x86.exe	NA	✓	✗
✗	MS06-070	Windows2000-KB924270-x86-ENU.E...	NA	✓	✗
✗	MS06-068	Windows2000-KB920213-x86-ENU.E...	NA	✓	✗

© 2006 AdventNet Inc. Server responded in 1863 milliseconds.

SecureCentral PatchQuest: Screenshot 2

secure | central™
PatchQuest

Feedback | About | Personalize | Help | License | Logout (admin)

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?

Quick Note

View missing and available patches for this system. The Product Summary presents a consolidated patch view of the products assessed in the system. You can select and "Deploy" the missing patches and "Undeploy" the available ones. Use the "Download" button to select and download required patches in to the server. >>

Scan Result > SD-TEST3

Scan Now Export Print Help

Deploy Download Undeploy Add To Patch Group Search None like Go

Showing : 1 to 25 of 60 Entries per page 25 Edit Column

Patch Status	Bulletin ID	Patch Name	Title	Installation Status	Download Status	Severity	Superseded By	Views
☐	MS05-037	New IES.01-KB903235-x86-ENU.exe	Vulnerability in JView Profiler Could Allow Remote Code Execution (903235)	NA		C	NA	
☐	MS05-036	New Windows2000-KB901214-x86-ENU.EXE	Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)	NA		C	NA	
☐	MS05-032	Windows2000-KB890046-x86-ENU.EXE	Vulnerability in Microsoft Agent Could Allow Spoofing (890046)	NA		M	NA	
☐	MS05-031	StepByStepInteractiveTraining-KB898458-x86-ENU.exe	Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (898458)	NA		I	NA	
☐	MS05-027	Windows2000-KB896422-x86-ENU.EXE	Vulnerability in Server Message Block Could Allow Remote Code Execution (026422)	NA		C	NA	
☐	MS05-011	Windows2000-KB885250-x86-ENU.EXE	Vulnerability in Server Message Block Could Allow Remote Code Execution (885250)	NA		C	NA	
☐	MS05-008	Windows2000-KB890047-x86-ENU.EXE	Vulnerability in Windows Shell Could Allow Remote Code Execution (890047)	NA		I	NA	
☐	MS05-003	Windows2000-KB871250-x86-ENU.EXE	Vulnerability in the Indexing Service Could Allow Remote Code Execution (871250)	NA		Y	NA	
☐	MS05-002	Windows2000-KB891711-x86-ENU.EXE	Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution (891711)	NA		C	MS05-018	
☐	MS05-001	Windows2000-KB890175-x86-ENU.EXE	Vulnerability in HTML Help Could Allow Code Execution (890175)	NA		C	MS05-026	
☐	MS04-044	Windows2000-KB885835-x86-ENU.EXE	Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (885835)	NA		I	NA	
☐	MS04-043	Windows2000-KB873339-x86-ENU.EXE	Vulnerability in HyperTerminal Could Allow Code Execution (873339)	NA		I	NA	
☐	MS04-041	Windows2000-KB885836-x86-ENU.EXE	Vulnerability in WordPad Could Allow Code Execution (885836)	NA		I	NA	

© 2005 AdventNet Inc.

Server responded in 125 milliseconds.

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. The interface includes a menu bar (File, View, Patches, Machines, Agents, Tools, Help), a toolbar, and a sidebar with navigation options like 'Patch Authority Ultimate Statistics' (showing 24,468 patches), 'Scan What' (My Machine, My Domain, My Test Machines, Entire Network), 'Favorites', 'Today's Items', and 'Recent Items'. The main pane shows a list of patches for 'JONDEMO2' and 'XPCUENT4'. The selected patch is 'Missing Patch Q935840 MS07-031'. The bottom pane provides detailed information for this patch, including its status (Missing Patch), vendor severity (Critical), CVEID (CVE-2007-2218), and a summary of the vulnerability in Windows XP Professional.

Type	QNumber	Item	Deployment	Pro
Missing Patch	Q935840	MS07-031	Wlr	Wlr
Missing Patch	Q935839	MS07-035	Wlr	Wlr
Missing Patch	Q935866	MS07-033	Wlr	Wlr
Missing Patch	Q932168	MS07-020	Wlr	Wlr
Missing Patch	Q931784	MS07-022	Wlr	Wlr
Missing Patch	Q931261	MS07-019	Wlr	Wlr
Missing Patch	Q930178	MS07-021	Wlr	Wlr
Missing Patch	Q929969	MS07-004	Wlr	Wlr
Missing Patch	Q929123	MS07-034	Wlr	Wlr
Missing Patch	Q928843	MS07-008	Wlr	Wlr
Missing Patch	Q928255	MS07-006	Wlr	Wlr
Missing Patch	Q927802	MS07-007	Wlr	Wlr
Missing Patch	Q927779	MS07-009	Wlr	Wlr
Missing Patch	Q926436	MS07-011	Wlr	Wlr
Missing Patch	Q926255	MS06-075	Wlr	Wlr

Patch Details

Status: Missing Patch
Install Patch

Vendor Severity: Critical
Criticality: Not Set
Add...

CVEID: CVE-2007-2218

Patch Download Status
English [X] 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

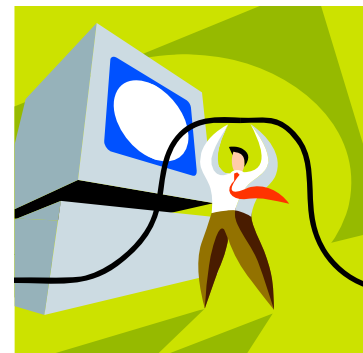
Summary
This critical security update resolves a privately reported vulnerability in the Secure Channel (Schannel) security package in Windows. The Schannel security package implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Internet standard authentication protocols. This vulnerability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

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

Novell ZENworks **PATCHLINK**

Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help | Server Time: 4/2/2004 11:14:23 AM (GMT-07:00)

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.

March 10, 2004
Microsoft Security Bulletin MS04-009

SEVERITY: Important

DATE RELEASED: March 9, 2004

SYSTEMS AFFECTED
Office XP SP2, Office 2002 SP2

RECOMMENDATION
Customers should install the patch at

Comprehensive Graphical Assessments:

Patch Status for all Reports



8.1%
66.9%
25.0%

Select to Change Graph:

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

patchlink

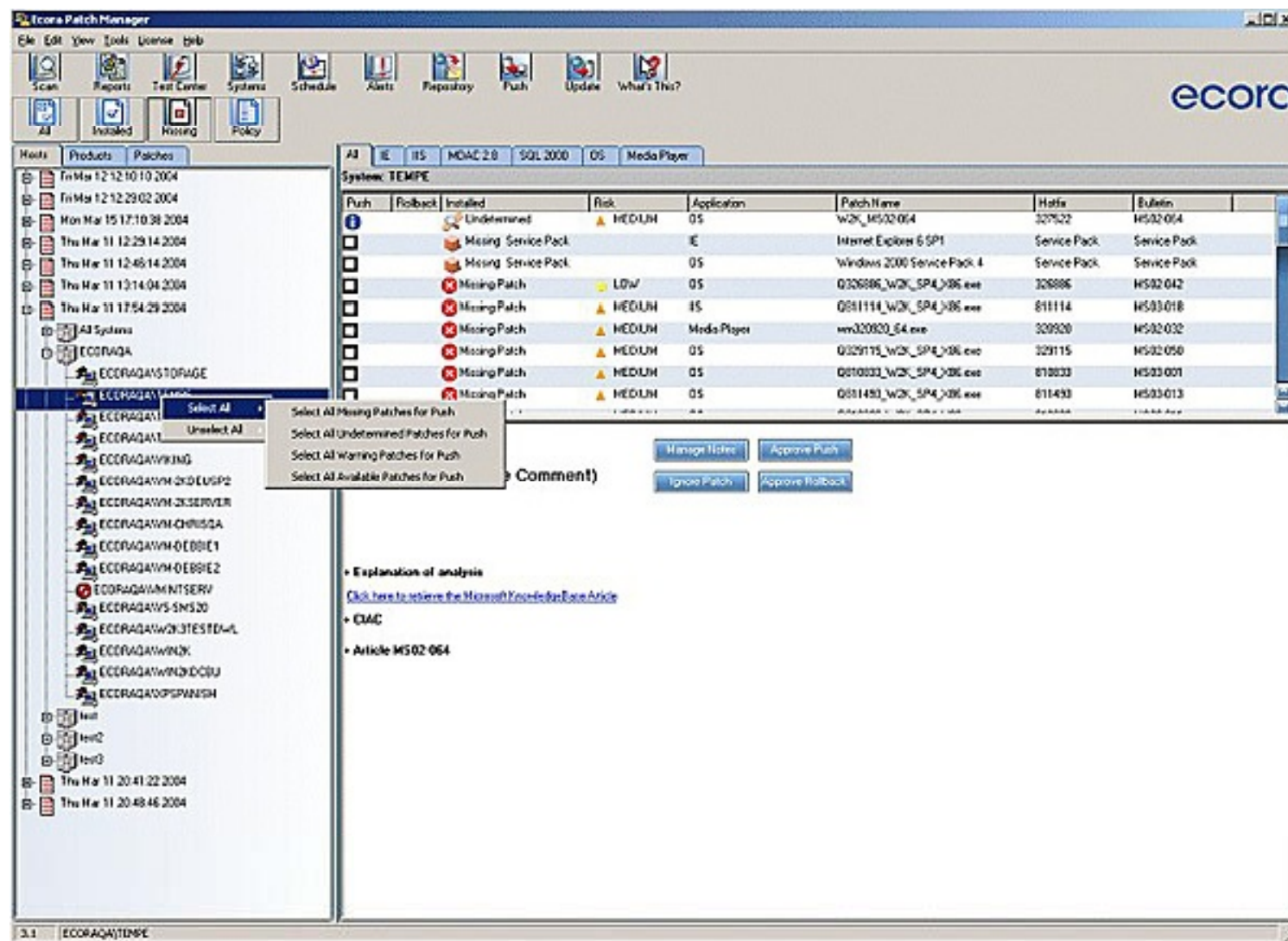
Tool: Ecora Patch Manager

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



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		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		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		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		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM

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



Tool: Altiris Patch Management Solution

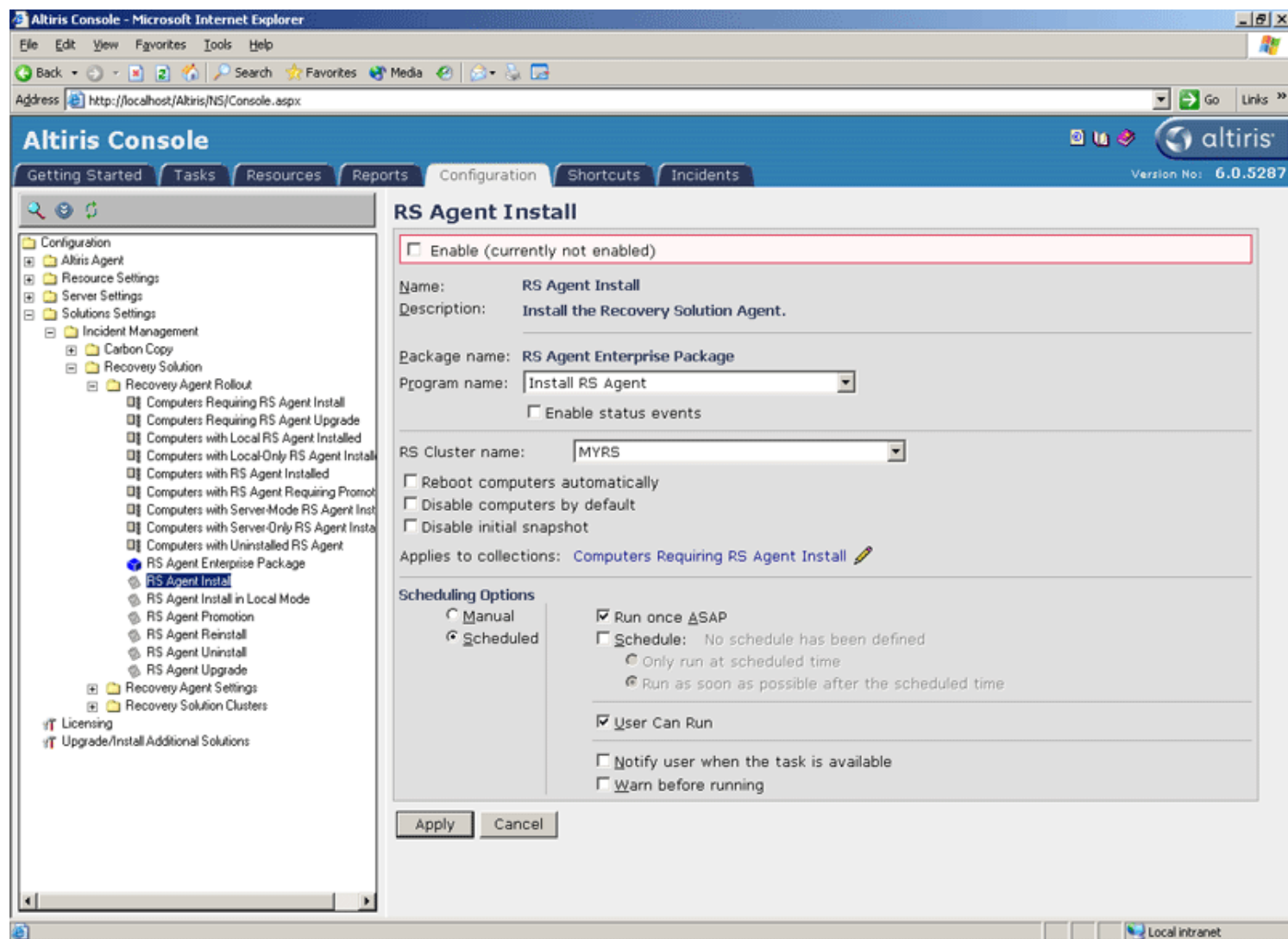
Altiris Patch Management Solution software proactively manages patches and software updates by automating the collection, analysis, and delivery of patches across your enterprise

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

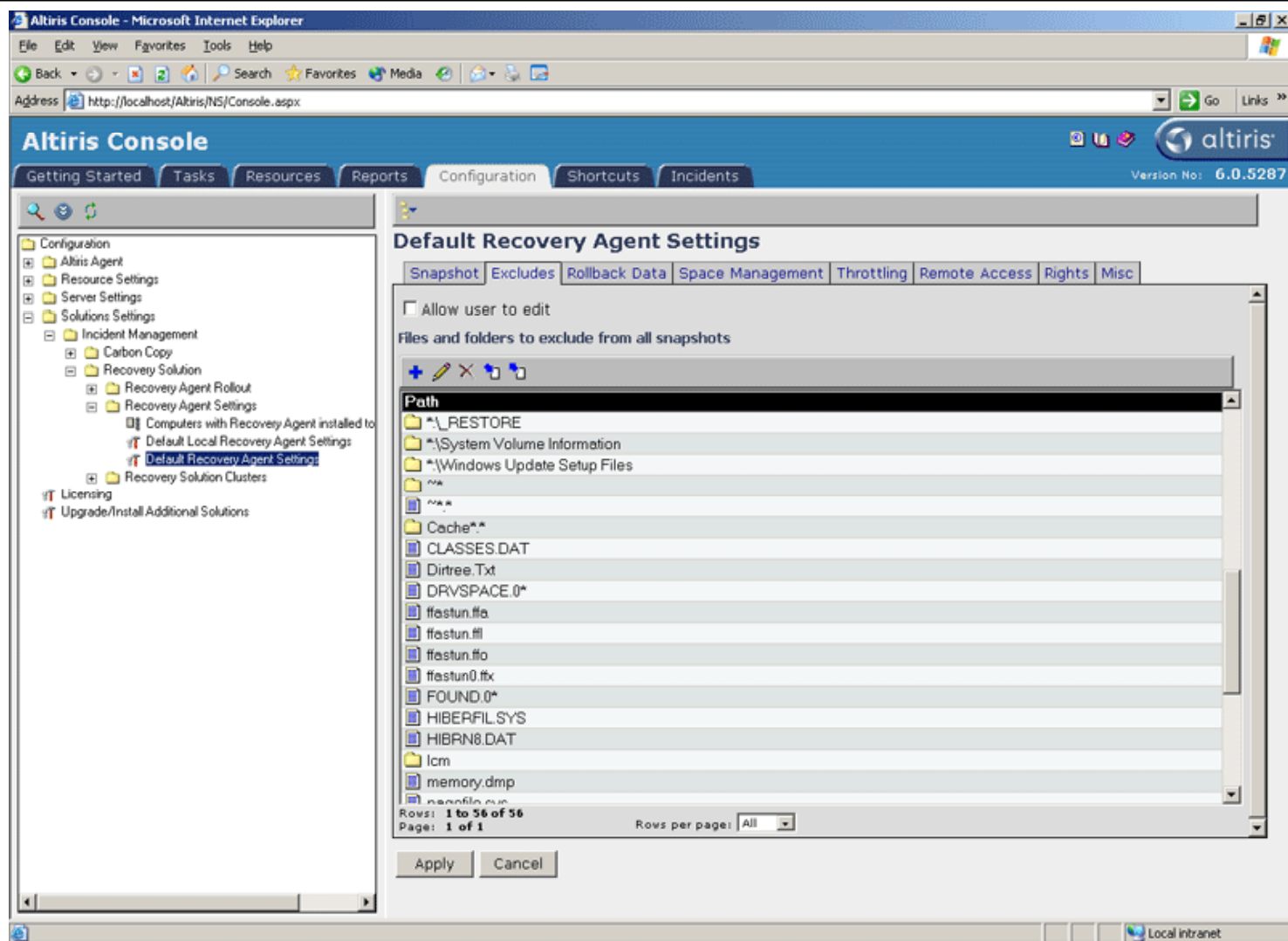
It provides improved functionality in the analysis, collection, and distribution of OS and application updates

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

Altiris Patch Management Solution: Screenshot 1



Altiris Patch Management Solution: Screenshot 2



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

BMC Patch Manager: Screenshot

BMC Configuration Management Report Center

Applications ▾ Common Tasks ▾ Home About Logout

Queries Query Library **Policy Compliance** Status Hide intro text Help

Compliance Target View

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.>

Targets previous 1-20 of 60 next

Search for: Go

☐ Do not search sub-containers

Home > Marimba > US

- Development
- Engineering**
- Finance
- Field Services
- HR
- IT
- Legal
- Marketing
- Office of CTO
- Purchasing
- Sales
- Support
- Training

Engineering View Policy

View compliance for: All policies affecting this target

Overall compliance: 70% 25% 25%

Policy last modified: 7/15/03 8:00AM
Members checked in: 400/500

Package	Policy State	Compliance	Directly Assigned To
Emacs	Install	80% 1% 19%	Engineering
Internet Explorer 6.0	Install	70% 400 22%	Mountain View
Trillian	Stage	100% 0% 0%	Mountain View
Visio	Advertise	100% 0% 0%	Engineering
WinZip	Install	90% 8% 8%	Mountain View

Green=Compliant Red=Non-compliant Blue=Not checked in

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



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 create baseline patch groups and scan 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

Numara Patch Manager

File View Patches Machines Tools Help

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...

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	Proje
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

Patch Details

Acrobat Reader 7.0.8 Adobe Reader 7.0.8

Status: Patch Found

Criticality: Not Set

Patch Download Status: English Download

Summary

The Adobe Reader 7.0.8 update adds new functionality, fixes a number of bugs, and is more secure. Adobe recommends that all Adobe Reader 7.0.x users apply this update.

Comments

Patch Info Missing Installed

110 Item(s)

Tool: TrueUpdate

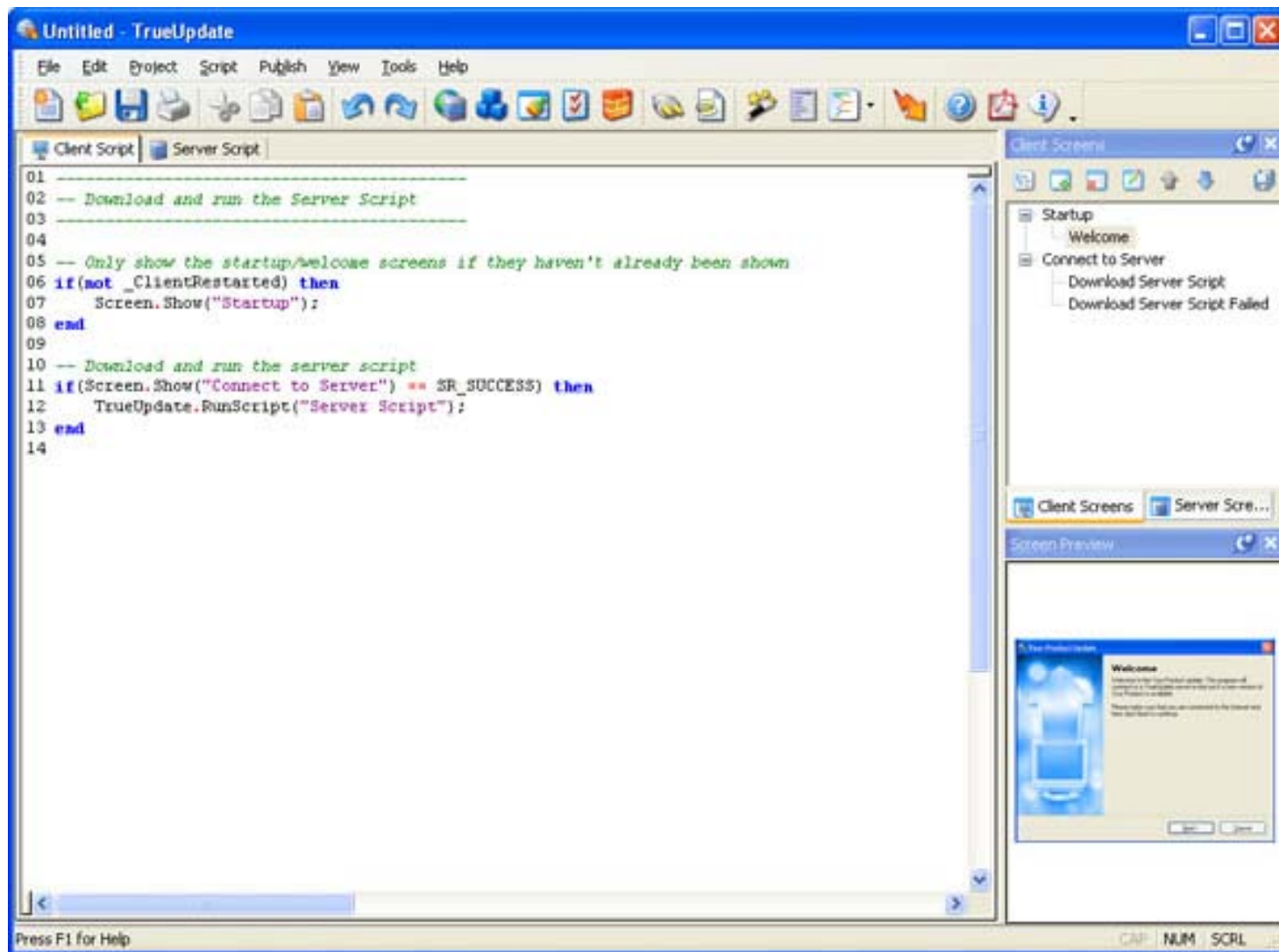
TrueUpdate is a comprehensive solution for software developers wanting to integrate automatic updating capabilities into their software applications

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

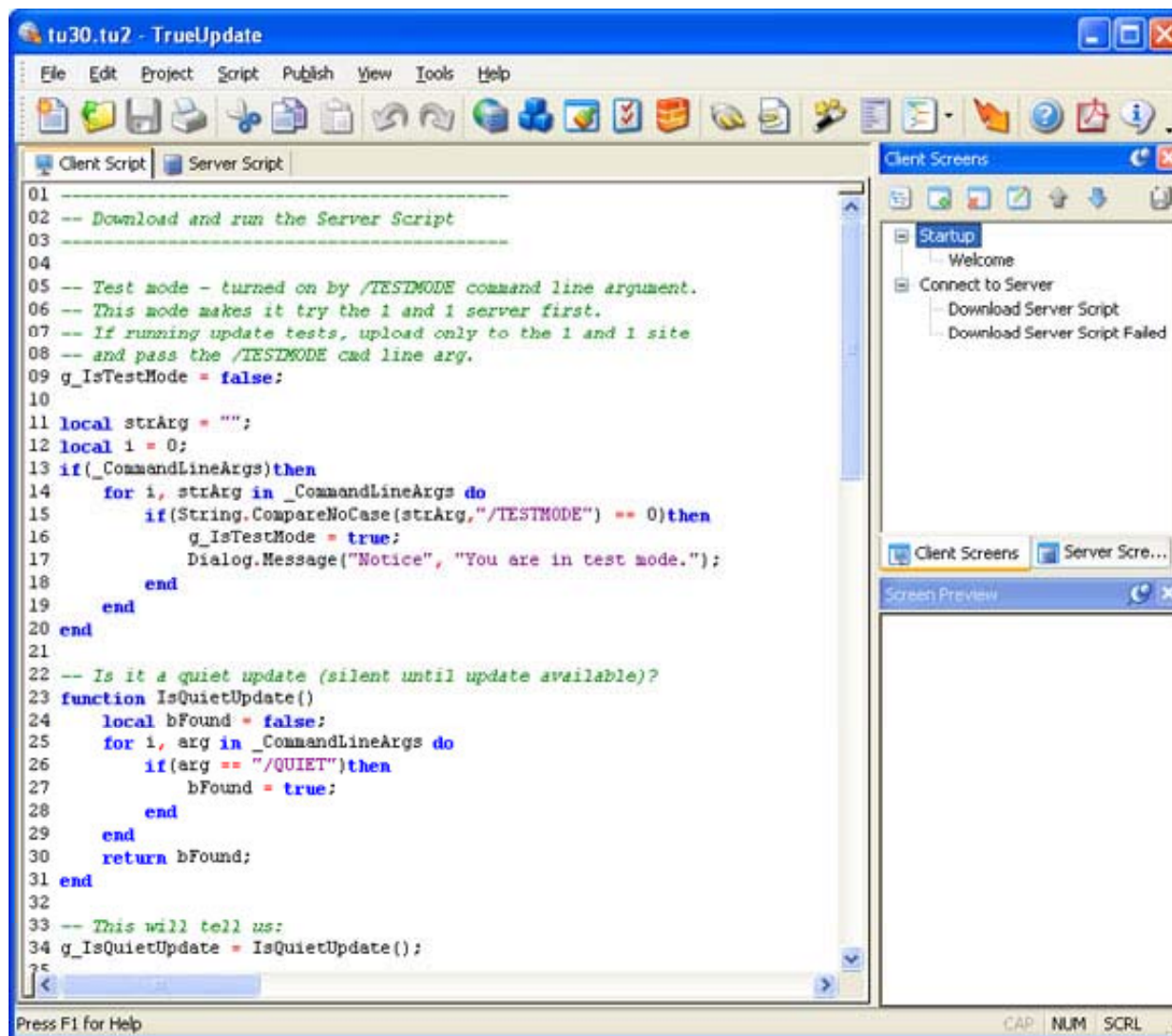
Features:

- 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

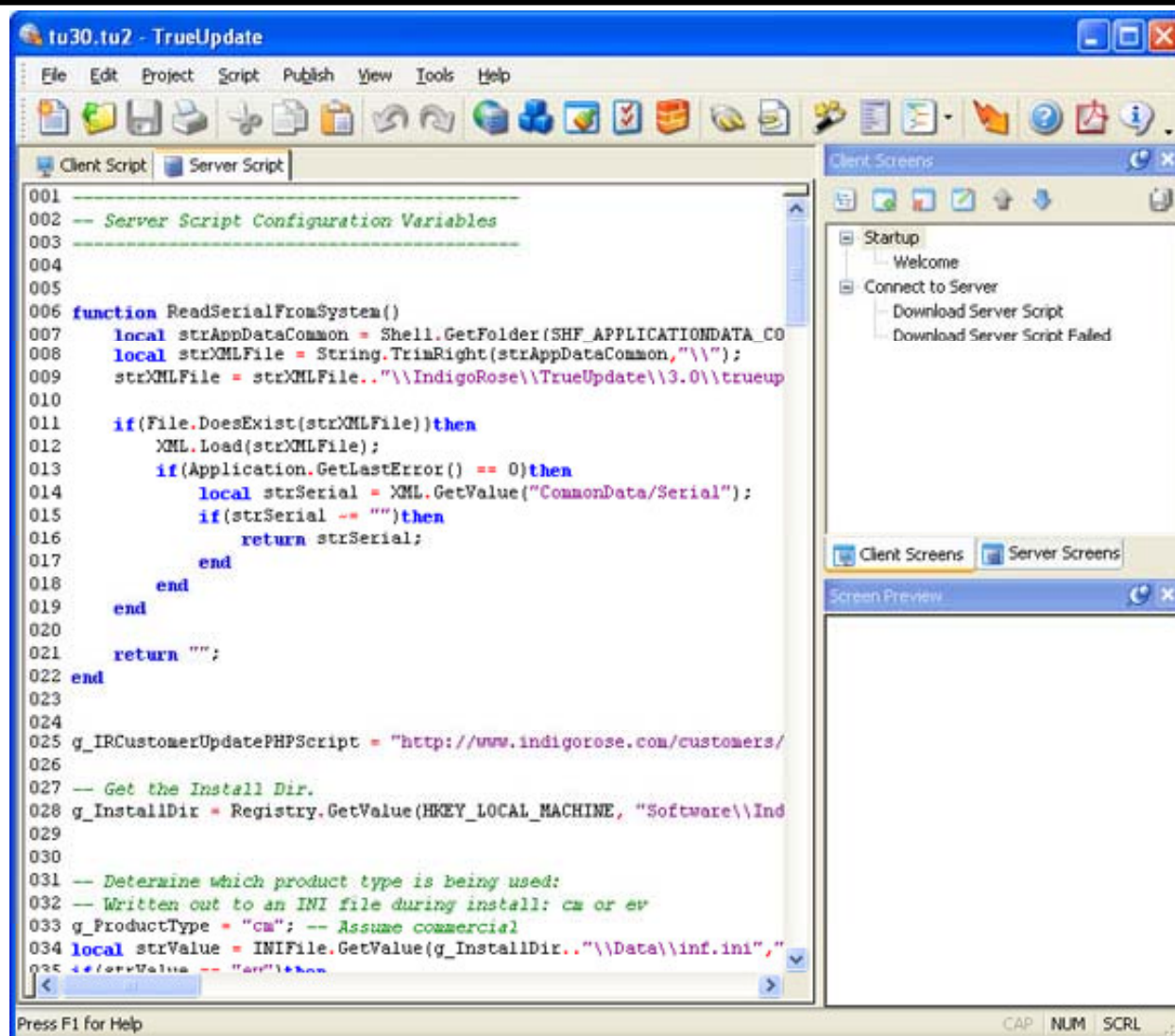
TrueUpdate: Screenshot 1



TrueUpdate: Screenshot 2



TrueUpdate: Screenshot 3



Tool: FlashUpdate

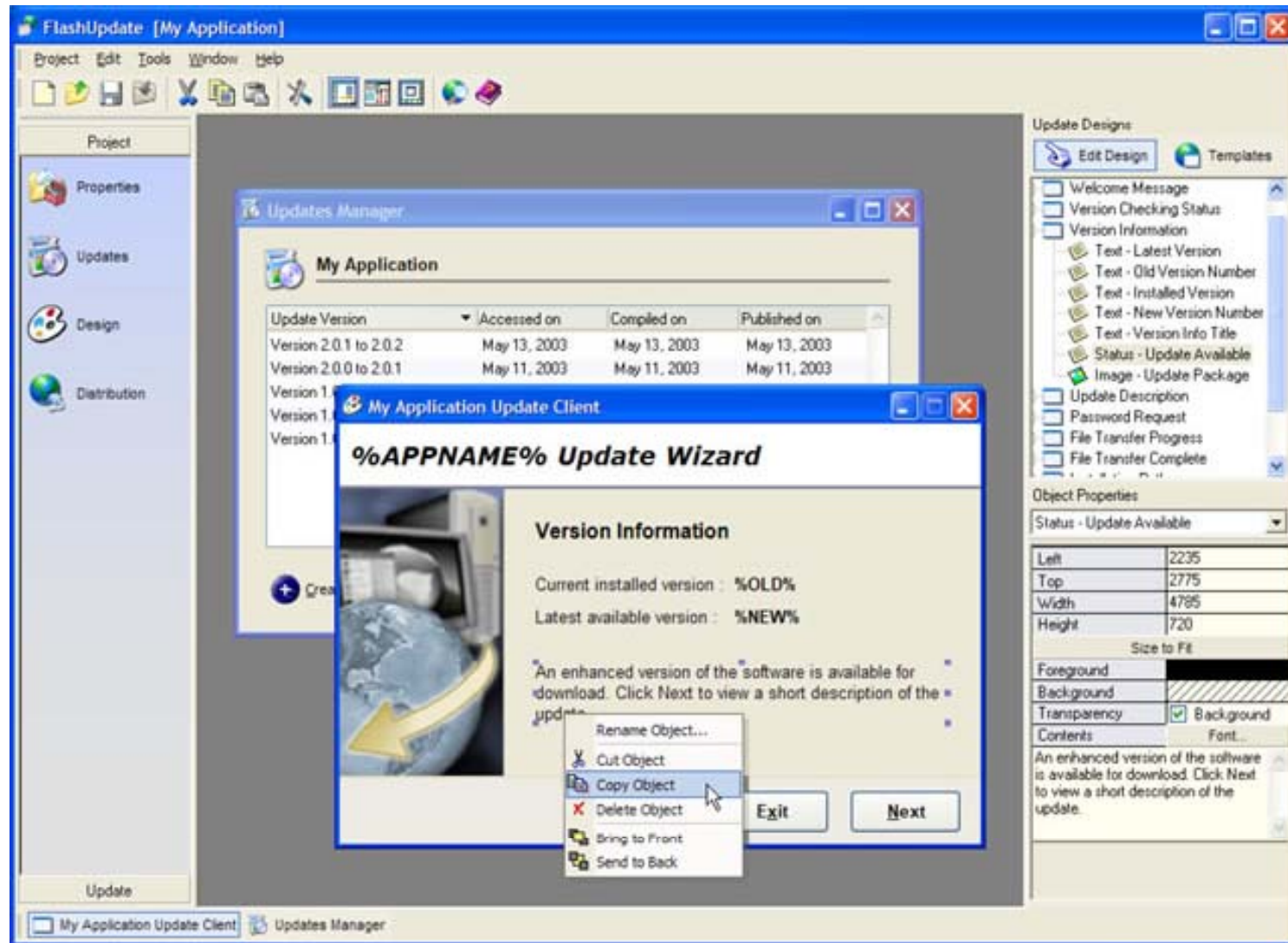
FlashUpdate is a software update solution for windows developers

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



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

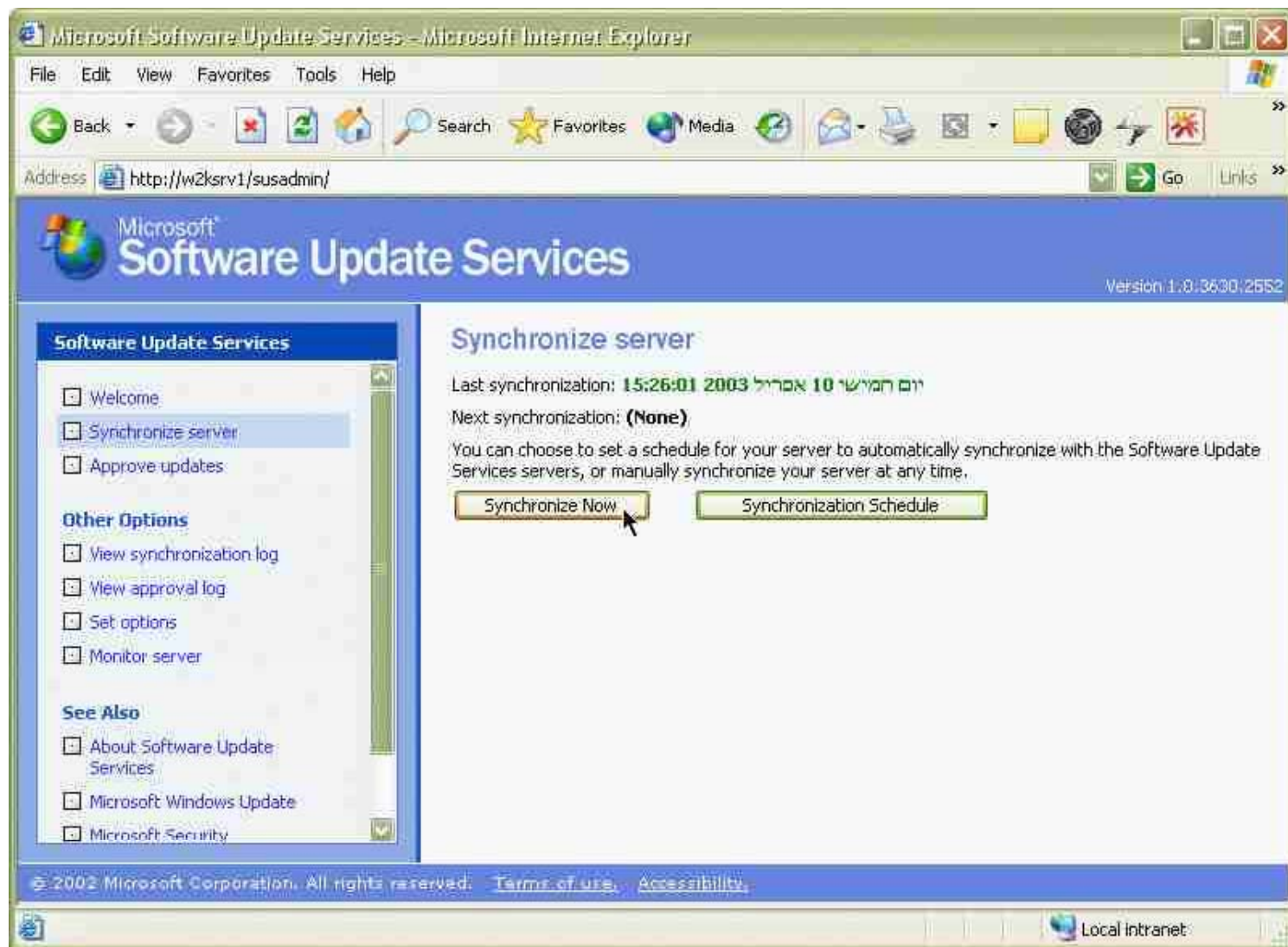
Administrators can receive e-mail notification when updates are added to their SUS pipeline

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



Microsoft Software Update Services (SUS): Screenshot 2



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

New Boundary Prism Patch Manager - Windows Internet Explorer

http://ppm

File Edit View Favorites Tools Help

New Boundary Prism Patch Manager

PRISM PATCH MANAGER

About | Log Out | Help

Server Date and Time: 2/20/2008 10:33:25 AM (UTC-06:00)

Home **Vulnerabilities** Deployments Devices Groups Users Reports Options

Name/CVE No: Status: Not Patched

Results for Groups: My Devices Impact: All

Include Child Groups: Show results on Page Load: Save as Default View: Update View

Vulnerabilities Packages

Vulnerability Name	Impact	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 wmfhotfi...	Critical - 05	0	1	0	0	1	100%
MS 887606 Update for MSXML 2.0 SP6	Recommend	0	1	0	0	1	100%
MS 887606 Update for MSXML 4.0 SP2	Recommend	0	1	0	0	1	100%
MS 909520 Microsoft Base Smart Card Cryptographic Service Provider Package	Recommend	0	1	0	0	1	100%
MS 909915 Patch 1 for installing Australian Daylight Saving time zones for year 2006 (SE...	Recommend	0	1	0	0	1	100%
MS 932590 DST update to C Runtime Library msqrt.dll for C applications	Recommend	0	1	0	0	1	100%
MS 941833 Update for Microsoft XML Core Services 4.0 Service Pack 2	Recommend	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%

Total: 114

1 of 2 Pages

Rows Per Page: 100

eric Deploy Disable Enable Export Update Cache Scan Now

Local intranet 100%

Prism Patch Manager: Screenshot 2

New Boundary Prism Patch Manager - Internet Explorer

http://wilbur/default.aspx?page=admin2

File Edit View Favorites Tools Help

New Boundary Prism Patch Manager

PRISM PATCH MANAGER

About | Log Out | Help

Server Date and Time: 3/12/2008 2:25:29 PM (UTC-05:00)

Home Vulnerabilities Deployments Devices Groups Users Reports **Options**

Subscription Products **Configuration** Policies E-Mail Support

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):

171 characters left.

Default Deployment Message (Max 256 Chars):

87 characters left.

eric Save Export

Done Local intranet | Protected Mode: Off 100%

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

Patch-Magic: Screenshot

patch_data.pbs - VisLogic Patch-Magic® V3.0

VisLogic Patch-Magic® V3.0

↑ update | search & scan | download & patch

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 Scannergebnisse
 - 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 Player
 - 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

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