

The Challenge

The volume and pace of newly discovered vulnerabilities is increasing every day, compelling security and IT professionals to reassess their approach to protecting large enterprise networks. According to the Computer Emergency Response Team (CERT) Institute "Over 99% of intrusions result from exploitation of known vulnerabilities or configuration errors where countermeasures were available." Hackers, viruses, and worms exploit these vulnerabilities, causing damage to information, disruption, and loss of service – driving up costs and preventing IT from focusing on strategic initiatives. The challenge IT faces is to gain the visibility and control across many thousands of distributed desktop, laptop, and server computers to:

- Detect and remediate these vulnerabilities
- Audit and report remediation status and current security posture
- Enforce secure configuration policies over time

Network and host-based scanning solutions can be effective at detecting vulnerabilities but have significant weaknesses including:

- Lack of real-time visibility to enterprise security posture due to periodic "scan interval"
- High false positive and false negative rate since detection is separated from remediation
- Lack of visibility into intermittently connected and remote computers
- Significant network bandwidth consumption
- Remote authentication and credentials are required for remediation

The Solution

The BES Vulnerability Management solution provides instant, proven fixes to many of the most common enterprise Windows computer vulnerabilities. Built upon the scalable, agent-based BigFix Enterprise Suite (BES) Platform, BES Vulnerability Management includes pre-packaged, pre-tested vulnerability detection and remediation that:

- Automates real-time vulnerability detection for Windows
- Dramatically reduces the time required to research, package, test and deploy fixes
- Automates enforcement of secure configuration for Windows computers
- Delivers real-time reporting on current vulnerability status, enterprise wide
- Eliminates redundant vulnerability detection tools by leveraging the existing BES infrastructure

With BES Vulnerability Management, detection and fixes to common vulnerabilities are delivered in real-time via the BES platform with BigFix Fixlet® messages (which provide the "intelligence" to identify vulnerabilities, a descriptions of the issues for the IT administrator, and the automated actions to apply and validate the fix).

- **SANS Top 10 Vulnerabilities to Windows Systems** – The ten most commonly exploited vulnerable services in Windows-based computers
- **Registry Vulnerability Solutions for Windows** – Detection and remediation for Windows vulnerabilities caused by common insecure Windows registry configuration
- **Security Policy Manager** - Detection and remediation of insecure browser configuration, email client configuration, removable media detection and prevention, network share detection, and more

Since BES Vulnerability Management leverages the real-time detection, reporting, and control delivered by the BES platform, there's no installation involved. No new scripting. No training. New security capabilities are up and running in a matter of moments.

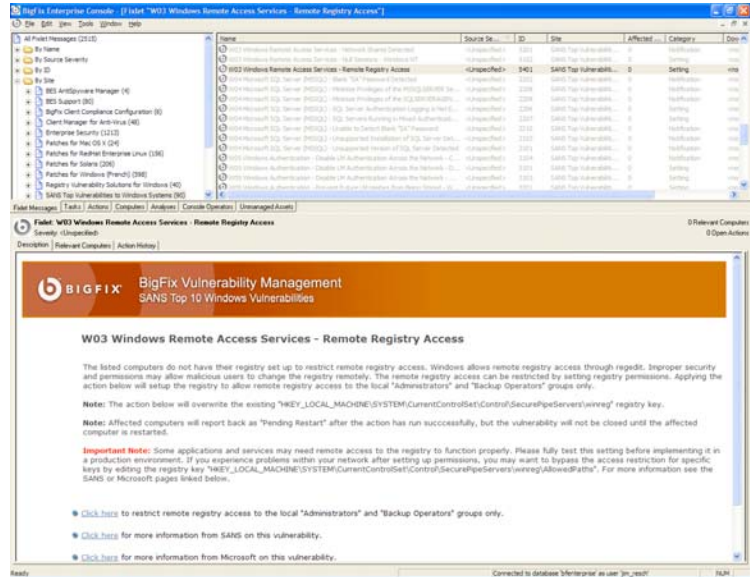
SANS Top 10 Vulnerabilities to Windows Systems

The vast majority of worms and other successful attacks are made possible by vulnerabilities in a small number of common operating system services. Each year, the SANS Institute and the National Infrastructure Protection Center at the FBI release a summary of the Ten Most Critical Internet Security Vulnerabilities for Windows Systems. This summary is a consensus of security experts of vulnerabilities that require immediate remediation for Windows computers. Many enterprises use the SANS summary to prioritize remediation efforts so that they can close the most dangerous vulnerabilities first.

Coverage of SANS Top 10 Vulnerabilities to Windows:

- W1. Web Servers & Services
- W2. Workstation Service
- W3. Windows Remote Access Services
- W4. Microsoft SQL Server
- W5. Windows Authentication
- W6. Web Browsers
- W7. File-Sharing Applications
- W8. LSAS Exposures
- W9. Mail Client
- W10. Instant Messaging

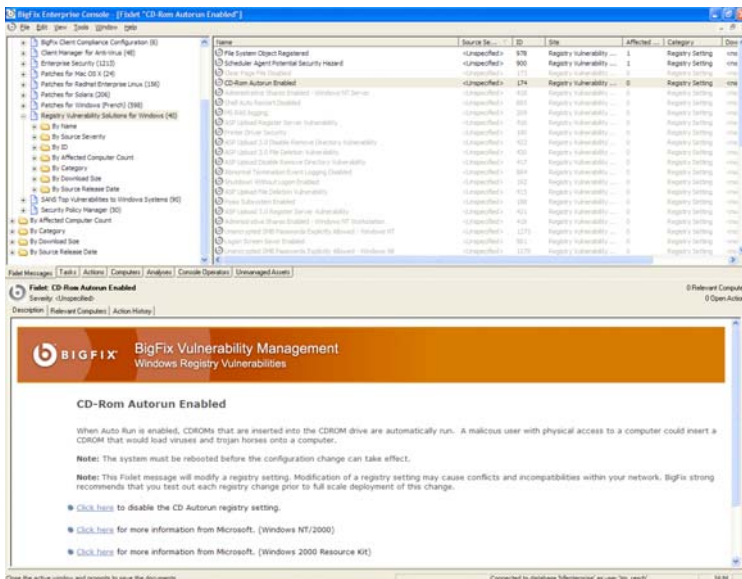
Including detection and remediation for common vulnerabilities including weak admin passwords, null sessions, IIS and SQL server mis-configurations and blank passwords, and P2P software.



Registry Vulnerability Solutions for Windows

Registry Vulnerability Solutions for Windows enables automated detection and remediation for Windows vulnerabilities caused by common Windows registry configuration issues, covering Windows 95, 98, NT, 2000, and XP. This Vulnerability Management solution address issues from 3rd party sources including:

- National Institute of Standards and Technology ICAT Metabase
- Microsoft Technet Security & Knowledge Base
- CERT Vulnerability Advisories



Detection and remediation of 40 vulnerabilities including:

- AEDEBUD registry key, MS00-008
- Allocate CDROMS, CAN-1999-0594
- Allocate floppies, CAN-1999-0594
- Anonymous registry, CAN-1999-0562
- Automatic admin logon, CAN-1999-0549
- CD-ROM auto run, CAN-2000-0155
- Exported registry files, CAN-1999-0572
- IP fragment reassembly, CVE-2000-0305
- Printer driver security, CAN-1999-0534
- Logon screen saver, CVE-1999-0382
- Shutdown without logon, CAN-1999-0593
- And More!

Security Policy Manager

Pre-packaged, pre-tested Fixlet messages that, in conjunction with BES, continuously monitor your Windows desktop, server, and laptop computers to ensure that they are compliant to security best practices and give you the ability to remediate simply and quickly non-compliant configuration. Security Policy Manager simplifies implementation and enforcement of secure configuration policies for the Windows OS, Internet Explorer, and Outlook.

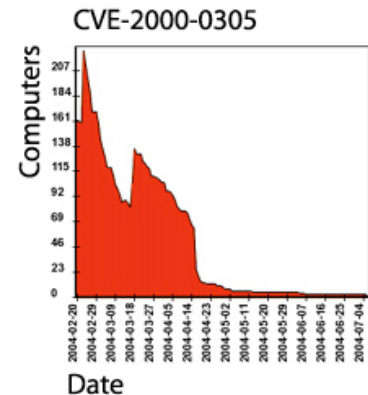
Detection and remediation of security best-practices including:

- IE secure configuration
- Outlook secure configuration
- Disable USB drives
- Screen Saver settings
- Clear system page file
- Enable encryption file System
- Network and administrative shares
- Unauthorized DHCP server
- Unauthorized DNS server
- Weak admin account password
- And More!

The screenshot shows the BigFix Enterprise Console interface. The top window displays a list of Fixlet messages with columns for Name, Source ID, Size, Affected, Category, and Download Size. The bottom window shows a detailed view of a 'Mobile Security: USB Storage Device Detected' message. The message content includes a description, a note about sensitive information, and several remediation actions such as 'Click here to instruct users to remove their USB storage devices' and 'Click here to prevent future use and to instruct users to remove their USB storage devices'.

BES Real-time Vulnerability Reporting

The BES platform provides a comprehensive set of real-time reports for enterprise wide assessment and trending of security posture and remediation progress. With BES Vulnerability Management and BES, security and IT professionals gain a centralized view of the current vulnerability and remediation status of all the computers in the enterprise.



About BigFix, Inc.

BigFix technology has received awards and recognition from numerous organizations and was recently named "Best New Security Solution for 2004" by *SC Magazine*, and is a finalist for the *Software & Information Industry Association's* Codie awards in both "Best Systems Management Solution" and "Best Security Product" categories for 2005".



BigFix, Inc.
 6121 Hollis Street
 Emeryville, California 94608
 [t] 510 652-6700
 [f] 510 652-6742
 [e] info@bigfix.com

Sales
 [t] 510 652-6700 x116
 [f] 510 652-6742
 [e] sales@bigfix.com

© 2005 BigFix® and the BigFix logo are registered trademarks of BigFix Inc. All other trademarks are the property of their respective owners. DS1006