

BigFix® Patch Manager

Data Sheet

With the exponential rise in security incidents, security experts and IT managers are under siege. Yet the vast majority of attacks can be prevented. According to Gartner Group, 90% of network attacks through 2005 will exploit security holes for which patches have been issued. An effective automated patch management solution is an essential component of enterprise security infrastructure.

BigFix® Patch Manager

BigFix Patch Manager accurately identifies machines that require security patches, and from a central console, mass-deploys them only where needed. It monitors the network to ensure patches remain intact and automatically redeploys them, increasing the security of the network while reducing costs and freeing up valuable IT resources for other high-priority initiatives.

Built on the powerful BigFix Enterprise platform, BigFix Patch Manager delivers superior network performance and scalability, managing thousands of machines from a single server. The software is easy and fast to install, deploy, and maintain and provides enterprise-class security, restricting access to only authorized personnel.

More importantly, BigFix Patch Manager will ensure 100% Microsoft® security bulletin compliance during the next security audit. It includes up-to-date Microsoft operating system and application patches released on the Microsoft TechNet or the Windows® Corporate Update Web sites.

BigFix Patch Manager is the only automated patch management solution optimized for large organizations.



- **BigFix Patch Manager** is the centerpiece of the BigFix Enterprise Suite, a set of solutions designed to dramatically improve the performance, security, reliability and manageability of large-scale networks. It includes:

- **BigFix Enterprise Server** — Stores and delivers up-to-date patches and updates and aggregates information from the client machines to a central database.

- **BigFix Enterprise Console** — A management interface for system administrators.

- **BigFix Enterprise Client** — A very small, efficient, and silent service running on each server, desktop, and laptop. Identifies required patches and manages deployment to the client machine.

- **BigFix Patch Manager Library** — A repository of pre-packaged patches for all critical HotFixes™, security updates, service packs, and virus-definition updates.

The screenshot shows the BigFix Enterprise Console interface. At the top, there is a table listing various vulnerabilities. One vulnerability, MS02-052, is highlighted. Below this, a detailed view of MS02-052 is shown, including an explanation of the vulnerability and an automated solution for deployment. At the bottom, a table lists the affected computers.

Name	Open Actions	Computers
MS02-044: Unsafe Functions in Office Web Components	2	2178
UPDATE: MDAC 2.7	0	2116
MS02-065: Buffer Overrun in Microsoft Data Access Components	2	1784
MS99-036: Windows NT 4.0 Does Not Delete Unattended Installation Files	0	1600
MS99-030: Office 95 ODBC Vulnerabilities	1	1415
MS02-052: Flaw in Microsoft VM JDBC Classes Might Permit Code to Be Run	1	1360
UPDATE: Internet Explorer 6.0 Service Pack 1 Available	0	1189
MS02-058: Unchecked Buffer in Outlook Express S/MIME Parsing - Outlook Express...	0	1147
MS02-032: 26 June 2002 Cumulative Patch for Windows Media Player 6.4	1	993

MS02-052: Flaw in Microsoft VM JDBC Classes Might Permit Code to Be Run

Microsoft has released a security bulletin outlining three new security flaws in Microsoft Virtual Machine build 3005. If correctly exploited, these flaws could allow a malicious user to take virtually any action on a user's computer. Microsoft recommends that all users running Microsoft Virtual machine apply this update.

Note: Affected computers will report back as 'Fixed' once the patch has run successfully, but the vulnerability will not be closed until the affected computer is restarted.

File Size: 167KB

Click here to initiate the deployment process.

Click here to view Microsoft Security Bulletin MS02-0052.

Computer Name	OS	User Name	CPU	Version of IE	RAM	Free Space on C:
FA178955	WinNT 4.0.1381	AC301SH	495 Mhz Pentium II	5.51.4807.2300	126 MB	4389 MB
FA215265	WinNT 4.0.1381	AC308ST	564 Mhz Pentium III	5.51.4807.2300	254 MB	5327 MB
FA249941	WinNT 4.0.1381	AC309BC	498 Mhz Pentium II	5.51.4807.2300	254 MB	5299 MB
FA249947	WinNT 4.0.1381	AC311ER	498 Mhz Pentium II	5.0.3105.105	254 MB	5165 MB
FA245630	WinNT 4.0.1381	AC315IK	498 Mhz Pentium II	6.0.2600.0	254 MB	3499 MB
FA249965	WinNT 4.0.1381	AC501NB	498 Mhz Pentium II	6.0.2600.0	254 MB	5528 MB



Patch Management: The Old Way vs. The BigFix Way

	The Old Way	The BigFix Way
Step 1: Risk Assessment	<ul style="list-style-type: none"> Monitor security sites for new vulnerabilities. Research vulnerabilities and patches, determine relevance of patch to the network. Run inventory reports to determine the number of machines affected. Assess exposure to the problem and prioritize which patches to deploy. Write code to package patches for deployment. 	<ul style="list-style-type: none"> BigFix provides immediate notification when patches are relevant and displays the affected machines. Click on link to read about known conflicts or deployment issues and access more detailed information.
Step 2: Testing and Packaging	<ul style="list-style-type: none"> Test packages on a subset of machines. Package code for mass deployment. Review inventory reports and manually group to target the affected machines. 	<ul style="list-style-type: none"> Test pre-tested, pre-packaged patches on a subset of machines.
Step 3: Deployment and Verification	<ul style="list-style-type: none"> Schedule off-hour deployment to limit network impact. Monitor process for failures. Run inventory reports again. Group failed machines and redeploy patches. Continue this cycle until all machines are patched. Run periodic inventory reports to verify compliance. 	<ul style="list-style-type: none"> Schedule a silent automated deployment with a few clicks and deploy only to affected machines. Monitors status as machines are fixed and gives notification of any problems during deployment. With a few clicks, redeploy a patch only where needed.
Step 4: Compliance Monitoring	<ul style="list-style-type: none"> Continue Step 3 until all machines are patched. Remember to manually patch new machines before they are added to the network. 	<ul style="list-style-type: none"> Console instantly reports machines out of compliance and automatically redeploys patches.
Step 5: Reporting	<ul style="list-style-type: none"> Accurate compliance reporting is too difficult. Deploy and ignore. 	<ul style="list-style-type: none"> Review system-wide reports to verify compliance. Sleep better at night.

BIGFIX PATCH MANAGER KEY FEATURES

Patch Intelligence

- Extensive library of patches: Microsoft-Complete HotFixes™, security updates, and service packs; virus updates from leading vendors
- Pre-packaged with information for relevance testing
- Hundreds of hardware and software features to accurately determine patch relevance
- Create custom patches and customize published patches with optional BigFix Development Environment

Deployment

- Automated targeting and deployment
- Automatic deployment of mandatory patches
- Delivers updates to remote machines whenever they log in
- Scheduled and time-based deployment
- Application and reboot control
- Network bandwidth throttling

Centralized Management and Administration

- Displays only relevant patches and affected machines
- Continuously monitors patches until every machine is repaired
- Displays detailed progress and real-time information -- no refresh required
- Comprehensive audit trail and patch history reporting

Architecture and Scalability

- Supports up to 5000 machines per server
- Remote network patch distribution through peer relay
- Low network overhead
- Small footprint client, low CPU usage

Enterprise-Class Security

- Robust security for administrative authorization, including digital signatures
- Big Fix Server rejects unsigned patches
- BigFix Client rejects unsigned patches

SYSTEM REQUIREMENTS

BigFix Enterprise Server:

- Windows 2000 Server
- Windows-compatible Web server
- TCP/IP network protected by a firewall
- Compatible with SQL Server, MSDE

BigFix Enterprise Console:

- Windows NT4+/2000/XP

BigFix Enterprise Client:

- Windows 95/98/ME/NT4+/2000/XP

CONTACT

BigFix, Inc.
5915 Hollis Street
Emeryville, CA 94608

t: 510.652.6700

f: 510.652.6742

www.bigfix.com

©2003 BigFix® and the BigFix logo are registered trademarks of BigFix, Inc. All other trademarks are the property of their respective owners.

