Release Notes for McAfee(R) VirusScan(R) Enterprise
Version 8.5i
Patch 6

==========

Patch Release: May 22 2008

This release was developed and tested with:

- VirusScan Enterprise: 8.5i
- DAT Version: 5288, May 5 2008
- Engine Version: 5.2.00

Make sure you have installed these versions, or later, before using this release.

==========

Thank you for using VirusScan(R) Enterprise software. This file contains important information regarding this release. We strongly recommend that you read the entire document.

The attached files are provided as is, and with no warranty either expressed or implied as to their suitability for any particular use or purpose. McAfee, Inc. assumes no liability for damages incurred either directly or indirectly as a result of the use of these files, including but not limited to the loss or damage of data or systems, loss of business or revenue, or incidental damages arising from their use. You are responsible for reading and following all instructions for preparation, configuration, and installation of Patch files. Patch files are not a substitute or replacement for product Service Packs which may be released by McAfee, Inc. It is a violation of your software license agreement to distribute or share these files with any other person or entity without written permission from McAfee, Inc. Further, posting of McAfee Patch files to publicly available Internet sites is prohibited. McAfee, Inc. reserves the right to refuse distribution of Patch files to any company or person guilty of unlawful distribution of McAfee software products. Questions or issues with McAfee Patch files should be directed to McAfee Technical Support.

WHAT'S IN THIS FILE

ABOUT THIS RELEASE

PURPOSE

This release contains updated binaries in a single Microsoft Patch installer to address all items listed in "Resolved Issues" below.

For the most update-to-date copy of this Readme information, refer to McAfee Support KnowledgeBase article 615747.

IMPROVEMENTS

1. The on-demand scanner has been updated to better use the System Utilization setting throughout the entire scanning process.

   Refer to McAfee Support Knowledgebase article 9197288 for further information.

2. This Patch contains a new Buffer Overflow and Access Protection DAT (version 378) which adds an Access Protection category for Virtual

Machine Protection. These rules provide access protection functionality for virtual machines.

NOTE:
In order to manage the new Virtual Machine Protection category with ePolicy Orchestrator 3.x or Protection Pilot, you will need to use the latest NAP file, included in this Patch package, or VirusScan 8.5i Repost Patch 5.

For ePolicy Orchestrator 4.x users, the Extension update also contains the updated rule file. The updated Extension package is available on the web product download area under the Patches category.

RESOLVED ISSUES

The resolved issues are divided into subsections per patch, showing when each fix was added to the compilation.

PATCH 6 RESOLVED ISSUES

1. ISSUE:
   The VirusScan Enterprise management plug-in writes all settings to the registry on every policy enforcement. McShield service monitors the registry and reloads whenever the settings are written, generating frequent pause events in the Windows System log.

   RESOLUTION:
   The VirusScan Enterprise management plug-in has been updated to only write to the registry if it sees that it is different from the current policy. This will prevent McShield from generating events on policy enforcement, unless that policy has changed.

   This is an addendum to the original solution in Patch 5, where the fix did not work when the preferred language was set to something other then automatic.

2. ISSUE:
   A compatibility issue has been seen with VirusScanís port blocking feature, and Veritas backup applications. This was causing the backup software services to stop running.

   RESOLUTION:

The VirusScan Anti-Virus Mini-Firewall Driver has been updated to correct the compatibility issue.

3. ISSUE:
A race condition in the On-Access Scanner service can cause high CPU utilization with high performance systems.

RESOLUTION:
The On-Access Scanner service has been updated to remedy multi-threading synchronization issues and remove occurrences of runaway threads.

4. ISSUE:
The On-Access Scanner service sometimes crashes during a system shutdown or during installation of a Patch/HotFix.

RESOLUTION:
The On-Access Scanner service has been repaired to correct a race condition in which a critical-section synchronization object is deleted before another thread has entered.

5. ISSUE:
A deadlock could occur on high end servers caused by a race condition in VirusScanís link driver.

RESOLUTION:
The link driver has been changed to properly handle the release of system objects, while holding a lock on resources.

6. ISSUE:
Port blocking fails on Microsoft Windows Vista Service Pack 1.

RESOLUTION:
The McAfee Driver Installer has been update to handle the changes in network stack load order.

7. ISSUE:
The On-Demand Scanner system utilization changes that were put in patch 5 changed the memory scanning function. This caused the process scanning to only scan the first process ID.

RESOLUTION:
The change has been reversed so that all processes are scanning irrespective of process ID.

8. ISSUE:
   When applied to a client installation that was customized by McAfee Installation Designer (MID), the patch installer deletes the MidFileTime registry value. This caused MID .CAB files to be re-applied to the system.

   RESOLUTION:
   The patch installer has been updated to no longer delete the MidFileTime registry value.

9. ISSUE:
   A newly created user defined Unwanted Program Policy, does not take affect immediately if the file has been scanned by the On-Access Scanner before the change occurred.

   RESOLUTION:
   The On-Access Scanner service has been updated to properly recognize changes to the user defined detections and clear the cache of files that have already been scanned so that the new settings take effect immediately.

10. ISSUE:
    A trust relationship exists in McAfee drivers that can be leveraged by McAfee processes to avoid triggering access protection rules and other compatibility symptoms. When the link driver was updated to newer releases this trust relationship was lost until a reboot occurred.

    RESOLUTION:
    The link driver has been modified to better handle the process of future upgrades to itself without the need for a reboot.

PATCH 5 RESOLVED ISSUES

1. ISSUE:
   Disabling the On-Access Scanner from the console is not always possible when users with sufficient privileges†belonged to large numbers of user groups.

   RESOLUTION:
   VirusScan Statistics has been updated so that users with sufficient privileges can now†disable the On-Access Scanner from the console regardless of how many user groups they belong too.

2. ISSUE:

The VirusScan Enterprise management plug-in writes all settings to the registry on every policy enforcement. McShield service monitors the registry and reloads whenever the settings are written, generating frequent pause events in the Windows System log.

RESOLUTION:
The VirusScan Enterprise management plug-in has been updated to write to the registry only if it sees that it is different from the current policy. This prevents McShield from generating events on policy enforcement, unless that policy has changed.

NOTE:
If the symptom persists, refer to McAfee Support KnowledgeBase article 614077.

3. ISSUE:
With the VirusScan Policy set to "Display managed tasks in the client console," the tasks sometimes disappear in the VirusScan Console.

RESOLUTION:
The On-Demand Scanner and Update console plug-ins have been updated so that when policy enforcement occurs, the console now updates the list of tasks to ensure an accurate display.

4. ISSUE:
When using system variables in the folder path for the Quarantine Manager Policy, the list of quarantined items is empty, even though items were quarantined to the correct directory.

RESOLUTION:
The Quarantine Manager console plug-in has been corrected so that the path specified in the folder input field is now properly expanded and the system variables are replaced before the list of Quarantined items is requested.

NOTE:
For further information about this fix, refer to McAfee Support KnowledgeBase article 614549.

5. ISSUE:
When a VirusScan Patch installation failed, the Help "About" dialog box no longer displayed the previous Patch number.

RESOLUTION:
The patch installer has been updated to write

the new Patch registry value only if the Patch succeeds. If it fails and a rollback occurs, the old Patch registry value remains.

6. ISSUE:
A 4E bugcheck (blue screen) can occur when VirusScan Enterprise 8.5i is installed along side SafeBoot Content Encryption 3.

RESOLUTION:
The link driver was updated to add supportability for SafeBoot.

7. ISSUE:
On Windows Vista and later, On-Demand Scan function "Save as Default" does not correctly save changes made for future scan tasks.

RESOLUTION:
The On-Demand Scanner has been corrected to properly save the registry data for the default task.

8. ISSUE:
Access Protection port blocking rules that spanned a range of ports could block all processes rather than only those processes specified in the rule.

RESOLUTION:
The Access Protection driver has been updated to better handle requests for process names.

9. ISSUE:
A 19 bugcheck (blue screen) occurred intermittently when loading and unloading content into Link Driver, for example, when configuration changes were made or enforced.

RESOLUTION:
The link driver was corrected to resolve a race condition that could lead to this issue.

PATCH 4 RESOLVED ISSUES

1. ISSUE:
A crash can occur on some systems when the On-Demand Scan Task includes the "Memory for rootkits" scan item.

RESOLUTION:
The root kit detection driver has been updated to better handle different processor

architectures.

2. ISSUE:
   When a Quarantine Restore Task is run from ePolicy Orchestrator without specifying a restore item, the Scan32.exe process runs a full scan and does not exit properly, leaving the process orphaned.

   RESOLUTION:
   The VirusScan plug-in has been updated to check if a restore item is specified. If not, the restore task does not run.

3. ISSUE:
   The VirusScan On-Demand Scanner has no option to disable cookie detection alerts in the user interface or registry.

   RESOLUTION:
   Alerts for On-Demand Scan cookie detections can now be disabled by setting the DWORD "bCookieAlerts" registry entry to 0.

   HKLM\SOFTWARE\McAfee\VSCore\Alert Client\VSE

4. ISSUE:
   When a user is browsing the Internet, the On-Access Scanner sometimes logs entries "Not scanned (The file is encrypted)" on temporary files that are locked for use by the browser.

   RESOLUTION:
   The reporting for these types of detections can now be disabled by setting the registry DWORD value "DoNotReportSkippedFiles" to 1.

   HKLM\SOFTWARE\McAfee\VSCore\On Access Scanner\McShield\Configuration

   NOTE:
   If you previously installed VSE85HF328421, the registry entry "DoNotReportSkippedFiles" is already set to 1.

5. ISSUE:
   In environments where the Lotus Notes data folder is in a non-standard location, the VirusScan Scanner for Lotus Notes installer might crash during installation of VirusScan.

   RESOLUTION:
   The VirusScan Scanner for Lotus Notes installation files have been updated so that the

search behavior for notes.ini is more resilient to custom Lotus Notes client locations.

6. ISSUE:
   A crash can occur, where the VirusScan Scanner for Lotus Notes failed to initialize properly if the first scanned attachment of a session was stored in a non-standard attachment format.

   RESOLUTION:
   The VirusScan Scanner for Lotus Notes library was changed so that the initialization code occurs before the attachment prefixed file name handling occurs.

7. ISSUE:
   With Self Protection enabled, the ability to unblock a connection from a remote computer is grayed out, even though the logged-on user has administrator privileges.

   RESOLUTION:
   VirusScan Statistics has been updated to check the credentials of the logged-on user, rather then the access level of our services, to determine if the "Unblock All Connections Now" button should be available.

8. ISSUE:
   Installation of this Patch enables the option "Enable on-access scanning at system startup" if it was previously disabled.

   RESOLUTION:
   The Patch installer has been corrected to properly preserve the setting.

9. ISSUE:
   The Patch installer returns a success code, even if the Patch failed to install.

   RESOLUTION:
   The Patch installer has been corrected so that it only returns a success code if it is actually successful.

10. ISSUE:
    Installing the Patch on a system that had only one Unwanted Programs exclusion causes that exclusion to fail.

    RESOLUTION:
    The installer now corrects a problem where the DetectionExclusions registry value was being

changed from REG_MULTI_SZ to REG_SZ if only one value existed.

11. ISSUE:
    On Windows Vista, the administrator cannot disable the On-Access Scanner via the VirusScan system tray icon.

    RESOLUTION:
    VirusScan Statistics has been updated to check the user's logged on credentials, rather then the service handle that was used to determine access to the McShield service in older operating systems.

12. ISSUE:
    A failed reinstallation of VirusScan or a failed Patch installation can delete the license, resulting in an inoperable product.

    RESOLUTION:
    The Patch installer has been updated to no longer cause this state in the event of a failed installation.

13. ISSUE:
    An incorrect rule file was packaged with the VirusScan NAP file included with Patch 3. This caused some of the Access Protection rule categories to not appear.

    RESOLUTION:
    A new VirusScan NAP file was created with a corrected rule file.

14. ISSUE:
    When Host IPS is installed with VirusScan Enterprise, and IPS is disabled, the interface for VirusScan Buffer Overflow Protection remains grayed out, even though it is active.

    RESOLUTION:
    The Buffer Overflow console plug-in was updated to check for the registry flag that is set by Host IPS, to tell VirusScan Enterprise that IPS is disabled.

15. ISSUE:
    When Self Protection is enabled on a remote machine and a user attempts open a remote console connection to that machine, the user receives an access denied message, and the remote console is not opened.

RESOLUTION:
The VirusScan Console was updated to make the connection to the remote console more robust.

PATCH 3 RESOLVED ISSUES

1. ISSUE:
A D1 bugcheck (blue screen) can occur with VirusScan Enterprise 8.5i when installed on heavily loaded servers.

RESOLUTION:
The Access Protection driver has been updated to resolve the issue.

2. ISSUE:
A D1 bugcheck (blue screen) can occur with VirusScan Enterprise 8.5i when installed on a Microsoft Exchange server.

RESOLUTION:
The Access Protection driver has been updated to resolve the issue.

3. ISSUE:
An 8E bugcheck (blue screen) was reported by customers and in Microsoftís Online Crash Analysis (OCA), showing a crash in an instruction that could not ordinarily fail.

RESOLUTION:
The Link Driver was revised to bring it into compliance with guidelines specified in Intelís Core2 Errata AI33, to prevent such unusual behavior on affected processors.

4. ISSUE:
A 7E bugcheck (blue screen) can occur with certain low resource conditions.

RESOLUTION:
The Link Driver has been updated to better handle scenarios where the system is low on resources.

5. ISSUE:
On 64-bit systems, VirusScan Statistics causes an issue where the user cannot open more then one Microsoft Virtual PC image. Virtual PC reports insufficient memory.

RESOLUTION:
VirusScan Statistics has been updated to resolve

a memory utilization problem on 64-bit systems.

6. ISSUE:
   When integrated with the Checkpoint SecureClient software, VirusScan Enterprise uses incorrect registry values for DAT and Engine version information.

   RESOLUTION:
   The binaries for Checkpoint integration have been updated to use appropriate registry data.

7. ISSUE:
   With Access Protections rules set to Maximum Security, during the installation, VirusScan Enterprise Checkpoint integration fails to query the On-Access Scanner service state.

   RESOLUTION:
   The binaries for Checkpoint integration have been updated to no longer request a certain level of access to the service, which would be denied by the higher level of Access Protection security.

8. ISSUE:
   Custom VirusScan Enterprise 8.5i policies are lost after upgrading from ePolicy Orchestrator 3.5 to 3.6.x.

   RESOLUTION:
   The VirusScan NAP file has been updated to include additional xml code for mapping policies between ePolicy Orchestrator 3.5 and 3.6.x.

   NOTE:
   To migrate the policies correctly, follow the instructions under "Installation Steps."

PATCH 2 RESOLVED ISSUES

1. ISSUE:
   When an AutoUpdate task copies new DAT files into the engine folder, VirusScan services and Microsoft Outlook can spike CPU utilization in excess of one minute.

   RESOLUTION:
   The McTaskManager service has been enhanced so that it no longer issues multiple reload notifications to the scanners after a DAT update.

NOTE:
Users who saw a smaller spike after the original fix (HF320829) should see more improvement with this fix.

2. ISSUE:
The Quarantine path cannot be changed for the On-Access Scanner via ePolicy Orchestrator or Protection Pilot. A registry value was not being updated correctly.

RESOLUTION:
VirusScanís Management Plug-In has been updated to correctly write the "RepairBackupDirectory" registry value.

3. ISSUE:
When creating a user-defined detection in the Unwanted Program policy, the rule does not take affect immediately. To enable the rule, the McShield service must be stopped and restarted.

RESOLUTION:
The McShield service has been updated to improve the monitoring of registry changes with the Unwanted Programs policy.

4. ISSUE:
VirusScanís ability to scan "floppy during shutdown" prevents proper shutdown of a system with a clean floppy in its drive.

RESOLUTION:
The On-Access Scanner has been updated to better handle the shutdown process.

5. ISSUE:
A crash was reported by customers and in Microsoftís Online Crash Analysis (OCA), during system start-up.

RESOLUTION:
The Link Driver was updated to correct synchronization issues during the start of processes.

6. ISSUE:
VirusScan does not correctly remove Buffer Overflow Protection process exclusions that are introduced by ePolicy Orchestrator or Protection Pilot.

RESOLUTION:
The VirusScan plug-in has been updated to

properly remove old Buffer Overflow Protection registry values when ePolicy Orchestrator or Protection Pilot policies are enforced.

7. ISSUE:
   When a detection occurs on an EMC network share (CAVA/Celera) and the file has the read-only attribute, the delete action fails.

   RESOLUTION:
   The Anti-Virus Filter and Link drivers where updated to properly remove the read-only attribute when taking action on files on the EMC share.

8. ISSUE:
   Detections on a network share may leave behind zero byte files on the share.

   RESOLUTION:
   The Anti-Virus Filter and Link drivers were updated to ensure proper cleanup of detections on a network share.

9. ISSUE:
   The On-Access Scanner functions in Console are not updating properly when Access Protection is disabled.

   RESOLUTION:
   The state of Self Protection is now correctly tracked by the On-Access Scanner Console plug-in.

10. ISSUE:
    The Self Protection feature of Access Protection is disabled after removing a Patch from the system.

    RESOLUTION:
    The MSP installer has been updated to fix a mismatched name between the custom action and installer execution sequence tables in the cached MSI file.

11. ISSUE:
    Interacting with Remote Console On-Demand Scan and AutoUpdate tasks caused the local tasks with the same id to be acted upon, instead of the remote task.

    RESOLUTION:
    The Update and On-Demand Scanner binaries were updated to properly call the remote task instead

of the local one.

12. ISSUE:
    When you upgrade from VirusScan Enterprise 7.1 or 8.0i to version 8.5i and choose to preserve settings, previously created console tasks do not display in the VirusScan console.

    RESOLUTION:
    The MSP Installer package has been updated to initialize the console tasks that were not previously initialized, so they display in the VirusScan console.

    NOTE:
    This fix is for those who used the originally released VirusScan Enterprise 8.5i. The current 8.5i repost package includes this fix.

13. ISSUE:
    With the McAfee Installation Designer (MID) option to "Allow Users to Uninstall" disabled, the UninstallString registry value was removed to prevent product removal. This registry value was also used by ePolicy Orchestrator to determine that VirusScan was installed.

    RESOLUTION:
    The VirusScan Detection Script has been updated to check for the existence of the uninstall key, instead of the UninstallString value, to determine if the VirusScan Enterprise install package needs to be pushed to the client.

14. ISSUE:
    Some threats were not being detected in the Quarantine Manager by the rescan functionality.

    RESOLUTION:
    The Common Shell Scanner binaries have been updated to resolve this issue.

15. ISSUE:
    If McShield and McTaskManager Services were stopped and restarted in a specific order, the Access Protection and Buffer Overflow features remained disabled after the services started.

    RESOLUTION:
    The On-Access Scan Console plug-in has been updated to recognize the last known state of Access Protection and Buffer Overflow Protection when McShield service is stopped.

16. ISSUE:
    McShield service may crash when a configuration change occurs during scanning.

    RESOLUTION:
    The McShield service has been updated to properly change states when altering configurations.

17. ISSUE:
    Setting a user interface password for Access Protection did not prevent the ability for the user to right-click and disable that feature. The option to disable right-click ability is under the "Other" category (Console and Miscellaneous).

    RESOLUTION:
    The password functionality has been moved to the BehaviorBlocking console plug-in so that the right-click option is now included with the Access Protection password options.

18. ISSUE:
    The Buffer Overflow Protection displays a detection in the On-Access Messages window when the "Show the messages when a buffer overflow is detected" option is disabled.

    RESOLUTION:
    The On-Access Scan Statistics binary has been updated to properly suppress the Buffer Overflow detection when configured to do so.

19. ISSUE:
    On-Access Scannerís Network Drive Scanning causes network copy times to increase, more then what is normally expected, when this option is enabled.

    RESOLUTION:
    The Common Shell binaries have been updated to no longer request a certain level of access to the network file(s), which would always be denied.

PATCH 1 RESOLVED ISSUES

1. ISSUE:
    Applications that perform operations with temporary files, such as printing, generate a "file missing" error.

RESOLUTION:
The link driver has been updated to correctly handle file operations that use the DeleteOnClose flag.

2. ISSUE:
When McAfee Policy Enforcer is pushed out to a system with VirusScan Enterprise 8.5i, McAfee trusted processes might trigger Access Protection rules. A reboot is required to correct the problem.

RESOLUTION:
The link driver has been revised to ensure trusted policies are propagated between instances of loaded drivers.

3. ISSUE:
Some files remain locked indefinitely. Third-party tools indicate that McShield.exe was leaking handles, thereby locking the file.

RESOLUTION:
The link driver has been updated to detect and handle the oplock break-in-progress status code and ensure file locks are released.

4. ISSUE:
Under certain conditions, VirusScan Enterprise scanner for Lotus Notes can mistakenly deny access to the Lotus Notes internal processes, if another Note is being accessed by the user. The message "You are not authorized to perform that operation" is displayed for the user.

RESOLUTION:
The Lotus Notes scanner binaries have been updated to resolve the issue.

5. ISSUE:
For non-English platforms, a control ID is displayed in the Status field of the On-Access Messages window, rather than the localized strings.

RESOLUTION:
The resource binary for the On-Access Scanner service has been updated to resolve this issue.

6. ISSUE:
When VirusScan Enterprise 8.5i is installed to Windows Vista 32-bit platforms, the Buffer Overflow Protection feature is not available.

RESOLUTION:
This Patch enables Buffer Overflow Protection for Windows Vista 32-bit environments.

7. ISSUE:
When a scheduled On-Demand Scan task fails to authenticate to a specified location, the user receives an erroneous error asking that VirusScan Enterprise be reinstalled.

RESOLUTION:
The localized binaries file has been updated to handle the specific event.

8. ISSUE:
ePolicy Orchestrator could fail to replicate distributed repositories when VirusScan Enterprise 8.5i is installed.

RESOLUTION:
The Common Shell binary has been updated to allow sharing of files with other processes.

9. ISSUE:
Users without local administrative rights are not able to use the Help file unless it was previously downloaded by an administrator.

RESOLUTION:
Non-administrative users can now download and use the current Help file.

10. ISSUE:
Not all VirusScan Enterprise events can be filtered in ePolicy Orchestrator reporting.

RESOLUTION:
The extended reports NAP file has been updated to allow filtering of all VirusScan Enterprise events.

11. ISSUE:
In certain circumstances, when a state change occurs with Access Protection, the On-Access Scanner cannot be disabled/enabled, and some Access Protection rules fail to log messages.

RESOLUTION:
The McTaskManager Service and Access Protection binaries have been updated to resolve this issue.

12. ISSUE:
When resuming from the hibernate state, the

system tray icon might be in the disabled state, reflecting the status of the On-Access Scanner. However, the scanner service is functioning normally.

RESOLUTION:
The system tray icon should always reflect the correct state of the On-Access Scanner when resuming from hibernation.

KNOWN ISSUES

1. The 5200 Engine must be installed prior to deploying Patch 5 or greater. The Patch updates the cached MSI tables to prevent a repair from restoring an unusable version of the engine. As a consequence, removal of the patch could result in restoration of the engine that was included in the original installation of VirusScan Enterprise 8.5i.

2. When checking an upgraded version of the VirusScan NAP or Extension into ePolicy Orchestrator the Unwanted Programs Policy, detection categories will all be re-enabled. You will need to disable the categories that you had set previous to the check-in. This is only an issue if the McAfee Anti-Spyware Module NAP or Extension was previously checked in.

3. Some customers have reported seeing VirusScan Statistics (VShield) crashing/disappearing from the system tray. Refer to McAfee Support KnowledgeBase article 613892 for more information on this issue.

4. If Host Intrusion Prevention 6.x or later is installed and disabled prior to VirusScan Enterprise, it is necessary to re-enable IPS and disable it again in order for VirusScan Buffer Overflow Protection to be properly enabled.

5. Sporadic crashes of the McShield Service have been seen during the patch install, on systems running McAfee AntiSpyware Enterprise Module. The service recovers correctly at the end of the patch process.

6. If you install this release interactively and cancel the installation on a system where a previous Patch was installed, after the rollback completes, the previous Patch no longer reports to ePolicy Orchestrator or appears in the "About

VirusScan Enterprise" window.

7. Installing the Patch and specifying a log file path using the Microsoft Installer (MSI) switch "/L" does not log to the specified path. A log file capturing full data is logged to the folder "McAfeeLogs" under the Temp folder.

8. If the Lotus Notes client is open when this release is installed, the installation completes successfully, but a reboot is required to replace the McAfee Lotus scanner files. The new files are not used until after a reboot.

9. Uninstalling VirusScan Enterprise Patches is now possible for computers running Windows Installer v3.x or later. This technology is not fully integrated for Windows 2000 operating systems, so there is no option to remove the Patch in Add/Remove programs. Please see instructions under "Removing the Patch" for removal via command-line options.

10. Uninstalling VirusScan Patches is not available for Windows NT platforms, because Windows Installer v3.x is not supported on this platform. The Patch still installs to all platforms supported by VirusScan Enterprise 8.5i.

11. Patches for VirusScan Enterprise 8.5i can only be uninstalled via Add/Remove programs, not via ePolicy Orchestrator or Protection Pilot.

FILES INCLUDED WITH THIS RELEASE

This release consists of a package called VSE85P6.ZIP, which contains the following files:

PKGCATALOG.Z =
   Package catalog file
PATCH6.TXT =
   This text file
VSE850DET.MCS =
   VirusScan Enterprise detection script
SETUP.EXE =
   Installer for this release
SETUP.INI =
   Initialization file for SETUP.EXE
PATCH6.MSP =
   Microsoft Installer Patch file
VSE850.NAP =
   Management NAP for VirusScan Enterprise

VSE850REPORTS.NAP =
Reporting NAP file

The following files are installed to client systems:

STRINGS.BIN	No version
NCEXTMGR.DLL	8.5.0.830
CONDL.DLL	8.5.0.857
COPTCPL.DLL	8.5.0.857
MCAVDETECT.DLL	8.5.0.869
MCAVSCV.DLL	8.5.0.869
NCDAEMON.EXE	8.5.0.886
NCINSTALL.DLL	8.5.0.886
BBCPL.DLL	8.5.0.895
CONSL.DLL	8.5.0.895
MCCONSOL.EXE	8.5.0.895
NCSCAN.DLL	8.5.0.895
SHUTIL.DLL	8.5.0.895
OASCPL.DLL	8.5.0.909
SHSTAT.EXE	8.5.0.909
FTCFG.DLL	8.5.0.913
MCUPDATE.EXE	8.5.0.913
NAIANN.DLL	8.5.0.913
QUARCPL.DLL	8.5.0.913
SCAN32.EXE	8.5.0.913
SCAN64.EXE	8.5.0.913
SCNCFG32.EXE	8.5.0.913
VSPLUGIN.DLL	8.5.0.913
VSODSCPL.DLL	8.5.0.913
VSTSKMGR.EXE	8.5.0.913
VSUPDCPL.DLL	8.5.0.913
ENTSRV.DLL	13.3.0.149
MFEAPFA.DLL	13.3.0.149
MFEAPFK.SYS	13.3.0.149
MFEAVFA.DLL	13.3.0.149
MFEAVFK.SYS	13.3.0.149
MFEBOPA.DLL	13.3.0.149
MFEBOPK.SYS	13.3.0.149
MFEHIDA.DLL	13.3.0.149
MFEHIDN.EXE	13.3.0.149
MFEHIDK.SYS	13.3.0.149
MFERKDA.DLL	13.3.0.149
MFERKDK.SYS	13.3.0.149
MFETDIK.SYS	13.3.0.149
ADSLOKUU.DLL	13.3.2.128
CSSCAN.EXE	13.3.2.128
ENTVUTIL.EXE	13.3.2.128
FTL.DLL	13.3.2.128
LOCKDOWN.DLL	13.3.2.128
MCSHIELD.DLL	13.3.2.128
MCSHIELD.EXE	13.3.2.128
MCSHIELDPERFDATA.DLL	13.3.2.128
MCVSSNMP.DLL	13.3.2.128

MYTILUS.DLL	13.3.2.128
MYTILUS2.DLL	13.3.2.128
NAEVENT.DLL	13.3.2.128
NAIEVENT.DLL	13.3.2.128
SCANOTLK.DLL	13.3.2.128
SCRIPTCL.DLL	13.3.2.128
SCRIPTSV.DLL	13.3.2.128
LOGPARSER.EXE	1.2.0.131

The following files are checked in to the ePolicy Orchestrator or ProtectionPilot repository:

VSE850.NAP	2.0.0.695
VSE850REPORTS.NAP	3.0.0.781

INSTALLATION AND REMOVAL

INSTALLATION REQUIREMENTS

To use this release, you must have VirusScan Enterprise 8.5i software installed on the computer you intend to update with this release.

NOTES:

- This release does not work with earlier versions of VirusScan software.
- A reboot is needed to fully load the system drivers into memory.†The package installation does not force the reboot.

INSTALLATION STEPS

1. Extract the Patch files from VSE85P6.ZIP to a temporary folder on your hard drive.

2. Double-click the file SETUP.EXE inside the temporary folder created in Step 1.

3. Follow the instructions of the installation wizard.

INSTALLATION STEPS VIA ePOLICY ORCHESTRATOR 3.x

1. On the computer where the ePolicy Orchestrator 3.x console resides, extract the Patch files and folders from VSE85P6.ZIP to a temporary folder on your hard drive.

2. Open the ePolicy Orchestrator 3.x console and

add the package from the temporary folder created in Step 1 to your repository.

Consult "Checking in Package" in the ePolicy Orchestrator 3.0 online Help, or "Checking in PKGCATALOG.Z product packages to the master repository" in the ePolicy Orchestrator 3.5 online Help, for instructions on adding a package to the repository. The package type for this Patch is "Products or Updates."

The next time an agent update task runs, the VirusScan Enterprise client automatically downloads and installs the Patch.

3. In the ePolicy Orchestrator console, add the VSE850.NAP file using the "Check in NAP" wizard.

   NOTE:
   The VSE850.NAP is the same as the one found in VirusScan 8.5i Patch 5 Repost. There is no reason to check it in again if you have already done so previously.

4. In the ePolicy Orchestrator console, add the VSE850Reports.NAP file using the "Check in NAP" wizard.

   NOTE:
   The VSE850Reports.NAP is the same as the one found in Patch 1. There is no reason to check it in again if you have already done so previously.

INSTALLATION STEPS VIA ePOLICY ORCHESTRATOR 4.x

1. On the computer where the ePolicy Orchestrator 4.x console resides, place the Patch archive VSE85P6.ZIP in a temporary folder on your hard drive.

2. Open the ePolicy Orchestrator 4.x console and add the VSE85P6.ZIP package from the temporary folder created in Step 1 to your repository.

   Consult "Checking in Packages Manually" in the ePolicy Orchestrator 4.0 online Help, for instructions on adding a package to the repository. The package type for this Patch is "Products or Updates (.ZIP)".

   The next time an agent update task runs, the

VirusScan Enterprise client automatically downloads and installs the Patch.

HOTFIX/PATCH REPORTING

Patch 4, and later, adds new functionality to the ePolicy Orchestrator properties for each computer. On the ePolicy Orchestrator Properties tab for each computer, the VirusScan 8.5i General branch displays two new entries:

- "Patch" displays the current Patch installed.

- "Fixes" displays any number of HotFixes listed in the registry.

A check is involved to verify that the HotFix/Patch matches the entry in the registry to the private build description of the HotFix binary. If the two donít match, the Patch or HotFix does not appear.

NOTE:
Currently there are no reports or compliance checks that use this new information.

MIGRATING POLICIES FROM ePOLICY ORCHESTRATOR 3.5 to 3.6

To migrate your policies correctly from ePolicy Orchestrator version 3.5 to version 3.6:

1. While still running ePolicy Orchestrator 3.5, install the VirusScan Enterprise 8.5 NAP file from Patch 3 or greater.

2. Upgrade to ePolicy Orchestrator 3.6. VirusScan Enterprise 8.5i policies will now appear to be missing/default.

3. Install ePolicy Orchestrator 3.6 Patch 2a or later.

   VirusScan Enterprise 8.5i customized policies should now be migrated and available.

VERIFYING THE INSTALLATION

Always reboot prior to validating that a Patch has installed successfully.

NOTE:
Patch releases do not display or report that the

Patch is installed if an error occurred during installation, or if a file or files did not install correctly.

1. Open the VirusScan Console and choose "About" from the "Help" menu. The "About VirusScan Enterprise" window "Installed Patches" displays "6."

   After property information has been collected by ePolicy Orchestrator and Protection Pilot agents, the client systems show that Patch 6 is installed as the "Hotfix" version. If the value "HotfixVersions" appears, it is a temporary value and will be removed after a full property collection from the client.

2. Confirm that the expected files are installed by checking the version number of individual files. File versions should match the list in "FILES INCLUDED WITH THIS RELEASE," above.

REMOVING THE PATCH

Windows Installer 3.x and later now support the rolling back of Patches. This can be done one of two ways.

- For Windows XP, Windows 2003, and Windows Vista operating systems, the Patch can be removed manually via Add/Remove Programs if the user has administrative rights to the local system.

- For all operating systems that support Windows Installer 3.x, a command-line option can be used to remove the Patch silently.

  Example:

  ```
  Msiexec.exe /I {35C03C04-3F1F-42C2-A989-A757EE691F65}
  MSIPATCHREMOVE={5DB77860-D5D2-4F0F-9118-6816878ACE0C} /q
  ```

  NOTES:

  - The GUID information used here will change from one Patch to another, so please use the information in the Release Notes for the patch that you are removing.
  - Because the patch is removed via MSIEXEC the functions inside setup.exe, that normally prevent reboots from occurring during silent processes, do not get executed. In order to prevent a possible automatic reboot from occurring after patch removal, simply add the REBOOT=R parameter to the command-line option

above.
- Patch removal is an MSI reinstall function. When a patch is removed, all features affected by the patch will get reset to installation defaults. Any features not modified by the patch will be left with their current settings.
- Update VirusScan after removing the patch to ensure that the latest versions of the Engine and virus definitions are run.

CONTACT INFORMATION

THREAT CENTER: McAfee Avert(R) Labs

Homepage
http://www.mcafee.com/us/threat_center/default.asp

Avert Labs Threat Library
http://vil.nai.com/

Avert Labs WebImmune & Submit a Sample (Logon credentials required)
https://www.webimmune.net/default.asp

Avert Labs DAT Notification Service
http://vil.nai.com/vil/signup_DAT_notification.aspx

DOWNLOAD SITE

Homepage
http://www.mcafee.com/us/downloads/

- Product Upgrades (Valid grant number required)
- Security Updates (DATs, engine)
- HotFix and Patch Releases
  - For Security Vulnerabilities (Available to the public)
  - For Products (ServicePortal account and valid grant number required)
- Product Evaluation
- McAfee Beta Program

TECHNICAL SUPPORT

Homepage
http://www.mcafee.com/us/support

KnowledgeBase Search
http://knowledge.mcafee.com/

McAfee Technical Support ServicePortal (Logon credentials required)

https://mysupport.mcafee.com/eservice_enu/start.swe

CUSTOMER SERVICE

Web: http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

Phone: +1-888-VIRUS NO or +1-888-847-8766
Monday-Friday, 8 a.m.-8 p.m., Central Time
US, Canada, and Latin America toll-free

PROFESSIONAL SERVICES

- Enterprise:
  http://www.mcafee.com/us/enterprise/services/index.html

- Small & Medium Business:
  http://www.mcafee.com/us/smb/services/index.html

LICENSE INFORMATION

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

LICENSE ATTRIBUTIONS

This product includes or may include:
*†Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). *†Cryptographic software written by Eric A. Young and software written by Tim J. Hudson. *†Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. *†Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. *†Software originally written by Robert Nordier, Copyright (C) 1996-7 Robert Nordier. *†Software written by Douglas W. Sauder. *†Software developed by the Apache Software Foundation (http://www.apache.org/). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt. *†International Components for Unicode ("ICU") Copyright (C)†1995-2002 International Business

Machines Corporation and others. *†Software developed by CrystalClear Software, Inc., Copyright (C)†2000 CrystalClear Software, Inc. *†FEAD(R) Optimizer(R) technology, Copyright Netopsystems AG, Berlin, Germany. *†Outside In(R) Viewer Technology (C)†1992-2001 Stellent Chicago, Inc. and/or Outside In(R) HTML Export, (C) 2001 Stellent Chicago, Inc. *†Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, (C) 1998, 1999, 2000. *†Software copyrighted by Expat maintainers. *†Software copyrighted by The Regents of the University of California, (C) 1996, 1989, 1998-2000. *†Software copyrighted by Gunnar Ritter. *†Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., (C) 2003. *†Software copyrighted by Gisle Aas. (C) 1995-2003. *†Software copyrighted by Michael A. Chase, (C) 1999-2000. *†Software copyrighted by Neil Winton, (C)†1995-1996. *†Software copyrighted by RSA Data Security, Inc., (C) 1990-1992. *†Software copyrighted by Sean M. Burke, (C) 1999, 2000. *†Software copyrighted by Martijn Koster, (C) 1995. *†Software copyrighted by Brad Appleton, (C) 1996-1999. *†Software copyrighted by Michael G. Schwern, (C)†2001. *†Software copyrighted by Graham Barr, (C) 1998. *†Software copyrighted by Larry Wall and Clark Cooper, (C) 1998-2000. *†Software copyrighted by Frodo Looijaard, (C) 1997. *†Software copyrighted by the Python Software Foundation, Copyright (C) 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org. *†Software copyrighted by Beman Dawes, (C) 1994-1999, 2002. *†Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek (C) 1997-2000 University of Notre Dame. *†Software copyrighted by Simone Bordet & Marco Cravero, (C) 2002. *†Software copyrighted by Stephen Purcell, (C) 2001. *†Software developed by the Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). *†Software copyrighted by International Business Machines Corporation and others, (C) 1995-2003. *†Software developed by the University of California, Berkeley and its contributors. *†Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http:// www.modssl.org/). *†Software copyrighted by Kevlin Henney, (C) 2000-2002. *†Software copyrighted by Peter Dimov and Multi Media Ltd. (C) 2001, 2002. *†Software copyrighted by David Abrahams, (C) 2001, 2002. See http://www.boost.org/libs/bind/bind.html for documentation. *†Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, (C) 2000. *†Software copyrighted by Boost.org, (C) 1999-2002. *†Software copyrighted by Nicolai M.

Josuttis, (C) 1999. *†Software copyrighted by Jeremy Siek, (C) 1999-2001. *†Software copyrighted by Daryle Walker, (C) 2001. *†Software copyrighted by Chuck Allison and Jeremy Siek, (C) 2001, 2002. *†Software copyrighted by Samuel Krempp, (C) 2001. See http://www.boost.org for updates, documentation, and revision history. *†Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), (C) 2001, 2002. *†Software copyrighted by Cadenza New Zealand Ltd., (C) 2000. *†Software copyrighted by Jens Maurer, (C)†2000, 2001. *†Software copyrighted by Jaakko J‰rvi (jaakko.jarvi@cs.utu.fi), (C)†1999, 2000. *†Software copyrighted by Ronald Garcia, (C) 2002. *†Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, (C)†1999-2001. *†Software copyrighted by Stephen Cleary (shammah@voyager.net), (C)†2000. *†Software copyrighted by Housemarque Oy <http://www.housemarque.com>, (C) 2001. *†Software copyrighted by Paul Moore, (C) 1999. *†Software copyrighted by Dr. John Maddock, (C) 1998-2002. *†Software copyrighted by Greg Colvin and Beman Dawes, (C) 1998, 1999. *†Software copyrighted by Peter Dimov, (C) 2001, 2002. *†Software copyrighted by Jeremy Siek and John R. Bandela, (C) 2001. *†Software copyrighted by Joerg Walter and Mathias Koch, (C) 2000-2002. *†Software copyrighted by Carnegie Mellon University (C) 1989, 1991, 1992. *†Software copyrighted by Cambridge Broadband Ltd., (C) 2001-2003. *†Software copyrighted by Sparta, Inc., (C) 2003-2004. *†Software copyrighted by Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications, (C) 2004. *†Software copyrighted by Simon Josefsson, (C) 2003. *†Software copyrighted by Thomas Jacob, (C) 2003-2004. *†Software copyrighted by Advanced Software Engineering Limited, (C) 2004. *†Software copyrighted by Todd C. Miller, (C) 1998. *†Software copyrighted by The Regents of the University of California, (C) 1990, 1993, with code derived from software contributed to Berkeley by Chris Torek.

V3.1.5