Issues resolved by hot fixes for OSCE 10.6 SP3

Critical Patch Build 5779

Issue 1: When starting the OfficeScan agent with POP3 email scanning enabled, the Real-time Scan (Ntrtscan.exe) service may not be able to start due to a timing conflict with the OfficeScan Listener (TmListen.exe) service.

Solution 1: This critical patch resolves the timing conflict by ensuring that the OfficeScan Listener service allows the RealTime Scan service to start before starting other services.

Issue 2: Under some situation, part of scanning process may hang and OfficeScan client may not be able to perform any action on the detected malware. When this happens, OfficeScan does not display a pop-up warning or generate a detection log.

Solution 2: This critical patch enables OfficeScan clients to perform the required action on malware detected under the scenario described above.

Issue 3: OfficeScan clients start firewall service improperly on the Microsoft(TM) Windows(TM) 8 and Windows Server 2012 platforms.

Solution 3: This critical patch updates the OfficeScan client files to ensure that clients correctly start firewall service.

Hot Fix Build 5756

Issue: The Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) features are not enabled automatically in some OfficeScan client modules.

Solution: This hot fix ensures that the DEP and ASLR features are enabled by default on all OfficeScan client modules.

Hot Fix Build 5757.1 replaced by Hot Fix Build 5779

Issue: OfficeScan clients cannot report the correct OfficeScan Data Protection service status to the server because some related files are missing and the wrong driver information is stored in the corresponding registry key.

Solution: This hot fix allows users to configure OfficeScan clients to reset the stored Trend Micro Data Loss Prevention(TM) service version information to trigger these clients to update

the Data Prevention package. This resolves the issue to ensure that OfficeScan clients report the correct OfficeScan Data Protection service status to the OfficeScan server.

Hot Fix Build 5757 replaced by Hot Fix Build 5779

Issue: OfficeScan clients that use IPv6 appear offline and with IPv4 addresses on the OfficeScan web console and the "IP Template" registry key does not work as expected.

Solution: This hot fix increases the buffer size for IPv6 information to ensure that the OfficeScan server can successfully retrieve the correct IPv6 address strings and that the "IP Template" key works normally.

Hot Fix Build 5758

Issue: The OfficeScan client packager tool cannot successfully generate an MSI package after users install OfficeScan 10.6 Service Pack 3 with Patch 1 Critical Patch 5712.

Solution: This hot fix ensures that the OfficeScan client packager tool can successfully generate MSI packages.

Hot Fix Build 5763 replaced by Hot Fix Build 5779

Issue: The OfficeScan client packager tool cannot successfully generate an MSI package after users install OfficeScan 10.6 Service Pack 3 with Patch 1 Critical Patch 5712.OfficeScan clients add a large number of logs to the "Tminstall.log" file each time the clients update the web reputation settings from the OfficeScan server.

Solution: This hot fix enables users to configure OfficeScan clients to add only the logs for the following two events to the "Tminstall.log" file:

- the TmIEPlugInBHO plug-in is installed for the first time
- the OfficeScan client is uninstalled

When enabled, this feature can help limit the size of the "Tminstall.log" file.

Hot Fix Build 5770

Issue: An issue prevents users from remotely installing OfficeScan clients from an OfficeScan server.

Solution: This hot fix resolves the issue so that the OfficeScan client remote installation works normally.

Hot Fix Build 5779

Issue 1: Before an OfficeScan agent runs an on-demand scan, it first checks the on-demand scan cache for files to exclude from the scan to reduce scanning time. Sometimes, on-demand scans take a long time to complete because some files may be scanned redundantly when the on-demand scan cache does not work properly.

Solution 1: This hot fix prevents this performance issue by updating the OfficeScan server and agent files.

Issue 2: The response of the OfficeScan server console slows down when a large number of OfficeScan clients upload firewall logs to the OfficeScan server at the same time. This can happen in any of the following scenarios:

- After a user notifies OfficeScan clients to send firewall logs by clicking the "Notify Client" button on the "Client Management > Logs > Firewall Logs" page while "Root" is selected.
- When OfficeScan clients are configured to send firewall logs frequently and the OfficeScan server manages a large number of clients.

Solution 2: This hot fix enables users to configure OfficeScan servers to regulate the number of requests for OfficeScan clients to send firewall logs when a large number of these requests are triggered at the same time. This can help ensure that the OfficeScan server console works smoothly under this scenario.

Hot Fix Build 5781

Issue: The link to the spyware log encyclopedia in OfficeScan is incorrect.

Solution: This hot fix updates the OfficeScan server file to connect to correct spyware encyclopedia link.

Hot Fix Build 5782

Issue 1: Under certain conditions, the OfficeScan Real-time Scan service may trigger a memory leak issue.

Solution 1: This hot fix prevents the memory leak issue.

Issue 2: The following may occur on OfficeScan clients that were installed by the OfficeScan Image Setup Tool (ImgSetup.exe) from a copied image file:

- the OfficeScan client icon appears in the system tray by mistake
- the OfficeScan client PccNtMon process does not work normally

Solution 2: This hot fix resolves these issues so that OfficeScan clients that were installed by the OfficeScan Image Setup Tool (ImgSetup.exe) from a copied image file work normally.

Hot Fix Build 5783

Issue: Sometimes, an issue with the exclusive control logic in the TmPfw and TmWfp filters may trigger both to register the TmWfp filter driver at the same time.

Solution: This hot fix updates the Network Security Components to ensure that the TmWfp filter driver can only be registered to either the TmPfw or TmWfp filter and not to both at the same time.

Hot Fix Build 5784

Issue: The Network Content Inspection Engine has been a part of the OfficeScan package since OfficeScan 10.6 Service Pack 2 Custom Defense Pack. However, blue screen of death (BSOD) occurs when this engine attempts to update the pattern while all the computer's non-paged pool memory is in use.

Solution: This hot fix prevents BSOD under the scenario described above.

Hot Fix Build 5804

Issue: When users query "Endpoint Virus/Malware Information" logs on the Trend Micro Control Manager(TM) web console, the scan type of Scan Now virus logs from OfficeScan servers appears as "N/A".

Solution: This hot fix enables OfficeScan to set the scan type of Scan Now virus logs to "ScanNow" to ensure that this.

Hot Fix Build 5805

Issue: Sometimes, the OfficeScan client TMUFE module cannot receive the complete chuck data while it attempts to communicate with an NTLM proxy server. When this happens, proxy authentication fails and the TMUFE module returns a -2407 error.

Solution: This hot fix resolves the issue by improving the logic and data-handling mechanism that the TMUFE module uses to communicate with NTLM proxy servers.

Hot Fix Build 5806

Issue: AutoCAD(TM) closes unexpectedly after users enable the Trend Micro Data Loss Prevention(TM) function on computers protected by OfficeScan 10.6 Service Pack 3.

Solution: This hot fix adds AutoCAD into the approved list to ensure that it works normally on computers protected OfficeScan 10.6 Service Pack 3 while the Data Loss Prevention function is enabled.

Hot Fix Build 5807

Issue: In the Ping Server function, the default location status for an OfficeScan client is "internal". Sometimes, an OfficeScan client automatically switches its location status from "external" to "internal" during startup even when there are no changes to its network settings. This may happen when the OfficeScan client cannot connect to the server during startup.

Solution: This hot fix ensures that OfficeScan clients update their location status using the correct registry key so that the location setting does not change unexpectedly during startup.

Hot Fix Build 5809

Issue: If multiple plug-in service (PLS) versions are available, the OfficeScan Control Manager Agent (CMAgent) reports the version and status information of all these available versions to the Trend Micro Control Manager(TM) server. This prevent the Control Manager server from determining which PLS version is currently installed on each OfficeScan client.

Solution: This hot fix sets a filter criteria to enable the OfficeScan CMAgent to report only the version and status information of the PLS version that is currently installed on the OfficeScan client to the Control Manager server.

Hot Fix Build 5813

Issue: Disabling the "Enable virus/malware scan" option in an OfficeScan client disables Scan Now, however, Scan Now may still run after updates when the "Perform Scan Now after update (excluding roaming clients)" option is enabled.

Solution: This hot fix ensures that Scan Now cannot be triggered when the "Enable virus/malware scan" Scan Now option is disabled even when the "Perform Scan Now after update (excluding roaming clients)" option is enabled.

Hot Fix Build 5814/5823

Enhancement: OfficeScan 10.6 Service Pack 3 Hot Fix 5729 allows users to unload OfficeScan clients through the "Client Management" page of the OfficeScan web console. This hot fix enables users to specify an automatic reloading interval for OfficeScan clients that have been unloaded through Hot Fix Build 5729.

Hot Fix Build 5815

Issue: Sometimes, an issue with the exclusive control logic in the TmPfw and TmWfp filters may trigger both to register the TmWfp filter driver at the same time.

Solution: This hot fix updates the Network Security Components to ensure that the TmWfp filter driver can only be registered to either the TmPfw or TmWfp filter and not to both at the same time.

Hot Fix Build 5816

Issue: When a user changes the computer name of an OfficeScan client that is registered to Trend Micro Control Manager(TM), the name information on the Control Manager console does not change.

Solution: This hot fix adds a function that automatically updates the OfficeScan client's computer name information on the Control Manager console after a user edits the computer name of the OfficeScan client.

Hot Fix Build 5821

Issue: Customer encountered a system hang caused by an issue with VSAPI. In some cases, Real-Time Scan may encounter an unhandled exception and IOTiCRCServer is suspended. In the meantime, scanning threads are waiting for IOTiCRCServer’s response, causing a system hang.

Solution: This hot fix releases updates an API so that the Real-time Scan service is able to close IOTiCRCServer during unhandled exception occurs. This API addresses the specified Real-Time Scan unhandled exception.

Hot Fix Build 5822

Issue: After installing Hot Fix 5769.u or later uninstall Hot Fix, users encounter the following error message while attempting to install the OfficeScan client using the autopcc.exe package with pre-scan enabled: "Unable to get pattern file. Contact your OfficeScan Administrator for

assistance". The reason is file path were changed while determine copy pattern file and cause copy file fail.

Solution: This hot fix resolves the issue by enabling autopcc.exe to reset the file path for pattern files after successfully copying pattern files during OfficeScan client installation.

Hot Fix Build 5822.1

Issue: When there are more than two versions of the Virus Pattern File in the OfficeScan client folder, the latest Virus Pattern File version may not appear on the client console.

Solution: This hot fix ensures that OfficeScan clients save only the two latest Virus Pattern File versions and promptly older versions after a successful update.

Hot Fix Build 5825

Enhancement 1: This hot fix enables the OfficeScan server to check if a client's UID exists in the database and to notify it to register again if it has no records of the client's UID.

Enhancement 2: This hot fix enables the OfficeScan server to keep the logs for an OfficeScan client when the UID does not exist in the database. The OfficeScan server will keep the logs for a specific number of days and sends the logs to Trend Micro Control Manager(TM) once the client has registered to the server and its UID is back in the database.

Hot Fix Build 5826

Issue: Sometimes, an OfficeScan client loads and updates the "tmpolicy.ptn" file at the same time instead of waiting for one task to finish before starting the next. When this happens, the Device Control Settings work abnormally.

Solution: This hot fix updates the Trend Micro Behavior Monitoring Service to ensure that OfficeScan clients do not attempt to load and upgrade the "tmpolicy.ptn" file at the same time.

Hot Fix Build 5827

Issue: The HTTPS connection sometimes cannot block a malicious URL. This issue may occur when the connection comes too fast and the thread is not initially ready. When this situation occurs, TMProxy may lose some connection.

Solution: This hot fix ensures that OfficeScan deploys Network Security Component (NSC) Hot Fix 5.82.1093 to Microsoft(TM) Internet Explorer (IE) and Mozilla Firefox browsers, which resolves this issue.

Hot Fix Build 5839

Issue: When the length of a Trend Micro Data Loss Prevention(TM) (DLP) log string exceeds the limit, the OfficeScan master service stops unexpectedly and will not be able to display DLP logs.

Solution: This hot fix updates some OfficeScan files to prevent the OfficeScan master service from stopping unexpectedly and ensure that OfficeScan can display DLP logs properly.

Hot Fix Build 5841/5843

Issue 1: An issue prevents users from installing the OfficeScan client's Network Security Components (NSC) drivers, "Tm_cfw.sys" and "Tmtdi.sys" on computers running on Microsoft(TM) Windows(TM) XP or Windows Server 2003.

Solution 1: This hot fix updates the OfficeScan client files to ensure that the NSC drivers can be successfully installed or upgraded on computers running on Windows XP or Windows Server 2003.

Issue 2: The OfficeScan client's Common Firewall Driver (TM_CFW.sys) may cause blue screen of death (BSOD) when the driver processes disordered TCP network packets.

Solution 2: This hot fix updates the OfficeScan client's Common Firewall Driver files to ensure that the disordered TCP packets can be processed successfully.

Hot Fix Build 5842

Issue: Older OfficeScan client versions do not report build numbers to the OfficeScan server, as a result, the OfficeScan web console displays the respective build numbers as "0" but can display the correct program version.

Solution: This hot fix updates the "DBserver.exe" file to ensure that older OfficeScan clients send the build numbers to the OfficeScan server and that the correct version and build numbers appear on the OfficeScan web console.

Hot Fix Build 5845

Issue: Sometimes, the Trend Micro TDI (TMTDI) driver which provides network traffic monitoring for the Web Reputation Server of OfficeScan agents may trigger performance issues on computers running on Microsoft(TM) Windows(TM) Server platforms.

Solution: This hot fix allows users to uninstall the TMTDI driver globally from all OfficeScan agents installed on any Windows Server platform.

Hot Fix Build 5849

Issue: The AEGIS module included in the OfficeScan agent may cause some processes to become unresponsive when the system resumes operation from sleep mode.

Solution: This hot fix updates the AEGIS module with the AntiHangLoose feature that resolves this issue.

Hot Fix Build 5851

Enhancement 1: This hot fix enables users to create a list of IPv4 addresses that Vulnerability Scanner (TMVS.exe) should exclude from vulnerability scans.

Enhancement 2: This hot fix enables users to configure the subnet mask and gateway of a network segment on Vulnerability Scanner (TMVS.exe) to validate whether it is possible to access that network segment. When enabled, this option allows the Vulnerability Scanner to skip the IP addresses under that network segment if the specific gateway is not available.

Hot Fix Build 5852

Issue: After installing a hot fix or patch, the OfficeScan agent from updating the build number in the corresponding registry key or may trigger it to update the information to the wrong value. As a result, the wrong build number appears in the "Windows Control Panel > Programs > Programs and Features > Version" tab.

Solution: This hot fix resolves the issue to ensure that OfficeScan 11 agents promptly and correctly update the build number information in the corresponding registry key after a successful hot fix or patch installation.

Hot Fix Build 5853

Issue: Sometimes, an OfficeScan agent encounters performance issues when its Damage Cleanup Services (DCS) (TSC.exe) checks the digital signature of files and the Microsoft(TM) Windows(TM) certificate on the agent computer is outdated.

Solution: This hot fix allows users to prevent DCS from checking digital signatures.

Hot Fix Build 5901

Issue: Sometimes the Trend Micro Active Update module does not delete unnecessary update folders from the "OfficeScan installation path¥Web¥Service¥AU_Data¥AU_Storage" folder.

Solution: This hot fix updates the Trend Micro Active Update module to ensure that it deletes unnecessary update folders from the "OfficeScan installation path¥Web¥Service¥AU_Data¥AU_Storage" folder.

The unnecessary folder delete action will be trigger in next successful update event. After the HF installation, please hold on until next OfficeScan server update.

Hot Fix Build 5902

Issue: Some domain names in OfficeScan client management are not consisted with the client registration information. This inconsistency causes the "Search for Computers" function to work incorrectly.

Solution: This hot fix updates the OfficeScan server and client files to resolve this domain name inconsistent issue.

Hot Fix Build 5904

Issue: OfficeScan Data Loss Prevention(DLP) function is not able to block HTTP/HTTPS POST on dlptest.com

Solution: This hot fix add the pattern of dlptest.com into blocking rule to make sure DLP can block HTP/HTTPS post on it.

Hot Fix Build 5907

Issue: An issue related to the TMFBENG module triggers the OfficeScan Tmlisten service to stop unexpectedly.

Solution: This hot fix updates the TMFBENG module to resolve the issue.

Hot Fix Build 5908

Issue: The OfficeScan NT Listener Service may not be able to start because the Trend Micro Active Update (AU) module cannot start successfully.

Solution: This hot fix allows users to enable the AU module to check certificates to help ensure that the module can start successfully.

Hot Fix Build 5911

Issue: An issue with the way OfficeScan handles scan threads may prevent users from transferring OfficeScan agents between OfficeScan servers, trigger an OfficeScan server to stop responding, or cause the NT RealTime Scan service to stop unexpectedly.

Solution: This hot fix updates the OfficeScan server and client files to resolve the scan thread handling issue.

Hot Fix Build 5921

Issue 1: The OfficeScan agent's Data Loss Prevention's (DLP) module blocks some documents even if it doesn't contain credit card information.

Solution 1: This hot fix updates the DLP module of the OfficeScan agent which has the latest dtSearch module to resolve file parsing bug of old dtSearch.

Issue 2: This hot fix enables Data Loss Prevention Endpoint SDK 5.7 to support up to version 45 and 46 of the Google Chrome(TM) web browser.

Solution: This hot fix updates the DLP module of the OfficeScan agent which supports up to version 45 and 46 of the Google Chrome(TM) web browser.

Hot Fix Build 5921.1

Issue: The OfficeScan agent's Data Loss Prevention's (DLP) module blocks some documents even if it doesn't contain credit card information.

Solution: This hot fix updates the DLP module of the OfficeScan agent which has the latest dtSearch module to resolve file parsing bug of old dtSearch.

Hot Fix Build 5923

Enhancement: OfficeScan servers deploy Common Firewall Pattern exception rules to all OfficeScan clients. By default, there are up to 5 server IP addresses allowed in GssTrustServer. This hotfix enables users to specify up to 40 server IP addresses for GssTrustServer.

Hot Fix Build 5931

Enhancement: This hot fix provides an option to enable the VSAPI feature on an OfficeScan server and to automatically deploy the setting to OfficeScan clients.

Hot Fix Build 5934

Issue 1: Sometimes, an OfficeScan client encounters performance issues when its Damage Cleanup Services (DCS) (TSC.exe) checks the digital signature of files and the Microsoft(TM) Windows(TM) certificate on the client computer is outdated.

Solution 1: This hot fix allows users to prevent DCS from checking digital signatures.

Issue 2: OfficeScan server may not be able to recognize token variables in the "Subject" field of C&C callback notification email messages. As a result, the token names appear instead of the corresponding information.

Solution 2: This hot fix ensures that OfficeScan server recognizes token variables in the "Subject" field of C&C callback notification email messages and replaces these variables with the correct information.

Hot Fix Build 5936

Issue: The OfficeScan Data Loss Prevention(TM) (DLP) module will generate a lot of logs when upload a large illegal file to webamil as attachment.

Solution: This hot fix provide a configuration let customer to set the time intervals to skip the logs generate by same file. The parameter "http_file_skip_time" is in dsa.pro, and it's default value is 1 (second).

Hot Fix Build 5937

Issue: The following occurs after users upgrade to OfficeScan 10.6 Service Pack 3 Patch 3:

- The "Scheduled Update" settings of the Integrated Server are grayed-out and when these settings are enabled, the update interval process takes longer than usual to complete.
- The "Manual Update" feature of the Smart Scan Pattern stops responding while updating components.

Solution: This hotfix updates the Integrated Smart Scan library link to resolve these issues.

Hot Fix Build 5939

Issue: The OfficeScan Server's Export function creates the list of exclusion list with new line feeds as CRCRLF.

Solution: This hot fix updates the Export function of the OfficeScan server to set correct new line feeds(CRLF) on the created exclusion list(WR_URL_List.csv).

Hot Fix Build 5940

Issue: Users may still be able to access web sites that the Trend Micro URL Filtering Engine (TMUFE) has failed to rate because of connection issues.

Solution: This hot fix provides a way for users to configure OfficeScan to automatically block access to web sites if the TMUFE cannot rate the web sites.

Hot Fix Build 5943

Issue: When an OfficeScan 10.6 Service Pack 3 client is configured not to upload firewall logs, it may automatically start uploading these logs after restarting.

Solution: This hot fix ensures that OfficeScan clients upload firewall logs only when enabled to do so.

Hot Fix Build 5944

Enhancement: This hot fix allows users to enable the customized update source option for specific OfficeScan clients through the OfficeScan web console. When this option is enabled, OfficeScan clients can update only from the specified update source for each.

Hot Fix Build 5949

Enhancement: This hot fix allows you to set ForceUseMapping option for specific OfficeScan clients. When this option is enabled, scanning network files will not affect system performance on OfficeScan client computers.

Hot Fix Build 5964

Issue: Users may not be able to run the SvrSvcSetup.exe tool using the "svrsvcsetup -enablessl" command to generate the Secure Sockets Layer (SSL) certificate on the OfficeScan server.

Solution: This hot fix changes the commands for generating certificates through the SvrSvcSetup.exe tool. This helps ensure that the tool works normally.

- To generate the SSL certificate for Microsoft(TM) Internet Information Services (IIS), run the following command:

  "SvrSvcSetup.exe –GenIISCert"

  A new SSL certificate is generated and is automatically added to the IIS SSL certificate store.

- To generate the SSL certificate for Apache(TM) Web Server, run the following command:

  "SvrSvcSetup.exe -GenApacheCert"

  A new SSL certificate is generated and is automatically added to the Apache SSL certificate store.

Hot Fix Build 5965

Issue: When users export "Scan Exclusion Lists" information for the settings of the following scan types from the "Client Management" screen of the OfficeScan web console, the generated CSV file will not contain any domain setting information for OfficeScan clients:

- Manual scans
- Real-time scans
- Scheduled scans
- Scan Now

Solution: This hot fix updates the OfficeScan server files so that OfficeScan exports the domain setting information for each OfficeScan client properly.

Hot Fix Build 5975

Issue: The Common Firewall version in the "Summary" page of the OfficeScan server console does not change after users upgrade to OfficeScan 10.6 Service Pack 3 Patch 3 with Critical Patch 5900.

Solution: This hotfix ensures that the latest Common Firewall version information appears in the "Summary" page.

Hot Fix Build 5977

Issue: On 32-bit OfficeScan clients running on 32-bit Microsoft(TM) Windows(TM) platforms, some file handles remain after OfficeScan runs a manual scan on a remote drive. This issue more commonly affects EMC storage devices.

Solution: This hotfix resolves this issue by enabling OfficeScan to use the same API set (VSAPI or AEGIS) for manual scans.

Hot Fix Build 5981

Issue: The AEGIS module of the OfficeScan 10.6 agent program may trigger some processes to close unexpectedly.

Solution: This hot fix updates the Behavior Monitoring Service module in OfficeScan 10.6 to ensure that the AEGIS module no longer triggers processes to close unexpectedly.

Hot Fix Build 5984

Enhancement: This hot fix allows users to enable the customized update source option for specific OfficeScan clients through the OfficeScan web console. When this option is enabled, OfficeScan clients can update only from the specified update source for each.

Hot Fix Build 5987

Issue: On OfficeScan clients, the time information in C&C callback logs is in the wrong format.

Solution: This hotfix ensures that the time information in C&C callback logs on OfficeScan servers and clients follows the correct format.

Hot Fix Build 5988

Issue: The OfficeScan TMListen service can detect only Update 3 of the Visual C++ Redistributable Package (VCRedist.exe).

Solution: This hotfix resolves this issue by enabling the OfficeScan TMListen service to use "Upgrade Code" instead of the "Product Code" to recognize VCRedist.exe because the product code may change after an update.

Hot Fix Build 5995

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring.

Hot Fix Build 5999

Issue: An issue related to the Behavior Monitoring Service module of OfficeScan 10.6 Service Pack 3 may cause blue screen of death (BSOD).

Solution: This hot fix updates the Behavior Monitoring Service module in OfficeScan 10.6 Service Pack 3 to prevent the BSOD issue.

Hot Fix Build 6008

Issue: OfficeScan clients display corrupted firewall profile information on the web console. The affected OfficeScan clients do not apply the correct firewall settings.

Solution: This hot fix ensures that the OfficeScan client uses the correct method of parsing firewall profiles. Local Pattern to solve the issue.

Hot Fix Build 6008.1

Issue 1: The "Ntrtscan.exe" process of OfficeScan agents may sometimes trigger performance issues due to handle leaks.

Solution 1: This hot fix resolves the OfficeScan client performance issue by correctly closing the handle leak.

Issue 2: The following policies of Trend Micro Behavior Monitoring Setting appear on the OfficeScan 10.6 server console after the server updates components through Control Manager. These policies does't work on OfficeScan 10.6 because Ransomeware feature is not supported.

- Ransomware: Invalid Host Process
- Ransomware: Associated Process
- Ransomware: Windows Host Process

Solution 2: This hotfix ensures that these policies do not appear on the policy list after the server updates components through Control Manager.

Issues resolved by hot fixes for OSCE 11.0

Hot Fix Build 1618

Issue 1: When the OfficeScan server updates OfficeScan agent settings to the database, the server purges old information without verifying the GUIDs for agents. As a result, OfficeScan agents that do not have a previous GUID entry in the database revert to default settings.

Solution 1: This hot fix adds a GUID checking mechanism that enables the OfficeScan server to verify if a particular agent GUID exists in the agent table of the database before updating the agent information. If a GUID does not exist in the agent table, the OfficeScan server returns an error message and does not overwrite the agent settings.

Issue 2: An unknown error occurs after users click the "Save" button on the "Global Client Settings" page of the OfficeScan web console.

Solution 2: This hot fix updates the OfficeScan program to ensure that users can successfully save changes to the "Global Client Settings" page of the OfficeScan web console.

Hot Fix Build 1619

Issue: When an OfficeScan server uses an SQL Server as a database, the "DbServer.exe" process stops unexpectedly if it encounters a null value in the agent domain information.

Solution: This hot fix updates the SQL procedure in the OfficeScan server program to enable "DbServer.exe" to handle null values properly.

Hot Fix Build 1620

Issue: A timing issue can cause the AutoPCC process and the OfficeScan agent TmListen or NtrtScan process to start at almost the same time. When this happens, component updates may fail because the TmListen or NtrtScan cannot be stopped.

Solution: This hot fix enables users to set how long the AutoPCC process should wait for the TmListen or NtrtScan to start before attempting to stop these processes which can help resolve the timing issue.

Hot Fix Build 1622

Issue: The client tree disappears from the OfficeScan web console when users attempt to create an OfficeScan user account using an Active Directory group and the group name contains a forward slash "/".

Solution: This hot fix ensures that the client tree displays correctly under the scenario described above.

Hot Fix Build 1623

Issue: When the OfficeScan server is in SQL mode, user accounts that have permission to specific domains on the OfficeScan agent tree do not receive notification email messages when violations are detected in agents under the corresponding domains.

Solution: This hot fix ensures that accounts that have permission to specific domains on the OfficeScan agent tree receives email notification messages when violations are detected in agents under the corresponding domains.

Hot Fix Build 1624

Issue: When Trend Micro Data Loss Prevention(TM) upgrades from version 5.7 to 6.0, the upgrade program does not stop the OfficeScan Data Protection Service which prevents it from overwriting some files. This causes the update to fail with some files successfully updated to version 6.0 while the rest remain in version 5.7. Under this scenario, blue screen of death (BSOD) occurs while the Data Loss Prevention agent applies the settings to the driver.

Solution: This hot fix enhances the Data Loss Prevention update program to ensure that it stops the OfficeScan Data Protection Service before running the upgrade.

Hot Fix Build 1625

Issue: If there are more than 10000 OfficeScan agents reporting to an OfficeScan server in SQL mode, it would take more than 60 seconds to display the dashboard on the OfficeScan web console.

Solution: This hot fix improves the way the OfficeScan web console retrieves the agent information from the database to ensure that it can display the dashboard without issues under the scenario described above.

Hot Fix Build 1626

Issue: OfficeScan clients are unable to receive the Device Control excepted program lists if clients have been assigned to get domain settings from an Update Agent.

Solution: This hot fix updates the OfficeScan client files to ensure that clients can receive the Device Control excepted program list from an Update Agent.

Hot Fix Build 1626.1/1805

Issue 1: A blank page appears when users attempt to access the Real-time Scan settings page on the OfficeScan web console.

Solution 1: This hot fix ensures that the Real-time Scan settings page on the OfficeScan web console displays properly.

Issue 2: When OfficeScan agent's setting, EnableCentralWhiteList, is disabled, after users modify the action setting for Real-time Scan on the OfficeScan web or agent console and save the change, Real-time Scan still uses the previous action setting.

Solution 2: This hot fix updates the OfficeScan server and agent files to ensure that Real-time Scan applies the action specified in the OfficeScan web or agent console.

Hot Fix Build 1628

Issue: The OfficeScan Master Service, "OfcService.exe", stops unexpectedly while managing OfficeScan tasks.

Solution: This hot fix updates the OfficeScan server files to resolve this issue.

Hot Fix Build 1629

Issue: The OfficeScan server program uses the HTTP GET method to handle firewall profile deletion and deployment. This method can handle only URLs that are shorter than 2083 bytes and returns a 404 error when users add a large number of firewall profiles.

Solution: This hot fix resolves the issue by enabling the OfficeScan server to use the HTTP POST method to handle the firewall profile list.

Hot Fix Build 1631

Issue: When users upgrade an OfficeScan 10.6 client installed by MSI package to OfficeScan 11 through the "Update Now" function, the value in the "DisplayVersion" registry key is not

updated promptly. When this happens, users will not be able to establish a VPN connection trough the Juniper network from the OfficeScan client computer.

Solution: This hot fix updates the value of the "DisplayVersion" registry key to ensure that users can successfully establish VPN connections through the Juniper network on affected computers.

Hot Fix Build 1633/1803

Issue 1: An issue related to the Behavior Monitoring Service module of OfficeScan 11.0 may trigger a memory leak issue.

Solution 1: This hot fix updates the Behavior Monitoring Service module in OfficeScan 11.0 to prevent the memory leak issue.

Issue 2: The OfficeScan agent "PccNTMon.exe" process may slightly increase OfficeScan's system memory usage in computers that have not been restarted for several days.

Solution 2: This hot fix improves the memory management mechanism of OfficeScan agents to keep the system memory usage within normal levels in computers that have not been restarted for several days.

Hot Fix Build 1635

Issue 1: Before an OfficeScan agent runs an on-demand scan, it first checks the on-demand scan cache for files to exclude from the scan to reduce scanning time. Sometimes, on-demand scans take a long time to complete because some files may be scanned redundantly when the on-demand scan cache does not work properly.

Solution 1: This hot fix prevents this performance issue by updating the OfficeScan server and agent files.

Issue 2: Users that do not have administrator privileges still have full access to the OfficeScan client program directory after users switch the OfficeScan client's security setting from "Normal" to "High".

Solution 2: This hot fix ensures that the OfficeScan client program automatically limits users that do not have administrator privileges to read-only access to the OfficeScan client program directory when the security setting is switched to "High".

Hot Fix Build 1636

Issue: An OfficeScan agent that acts as an Update Agent can be configured to update components from the OfficeScan server only, however, Update Agents cannot be configured to update the domain settings only from an assigned OfficeScan server.

Solution: This hot fix updates the OfficeScan server and agent files to ensure that Update Agents can be configured to update components and domain settings only from an assigned OfficeScan server.

Hot Fix Build 1637

Issue: The information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan (Scan Now)" fields on the "Agent Management" page of the OfficeScan web console are not updated after a Manual Scan or a Scan Now task completes.

Solution: This hot fix updates some OfficeScan files to ensure that the information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan (Scan Now)" fields on the "Agent Management" page of the OfficeScan web console are updated promptly after each virus scan task.

Hot Fix Build 1638

Issue: When users trigger the "Scan Now" feature of an OfficeScan agent to run a manual scan, some drives do not appear in the scan folder selection box.

Solution: This hot fix updates some OfficeScan files to ensure that the scan folder selection box displays all drives under the scenario described above.

Hot Fix Build 1639

Issue: OfficeScan agents that are assigned to a customized update source list download components by matching IP addresses to the corresponding IP range. If an agent binds multiple IP addresses, the agent program may not be able to enumerate all bound IP addresses which prevents it from downloading components.

Solution: This hot fix updates the OfficeScan server and agent files to ensure that OfficeScan agents with bound multiple IP addresses can successfully enumerate all these addresses when downloading components from customized update sources.

Hot Fix Build 1641

Issue: Under specific US Trend Micro Data Loss Prevention(TM) templates, OfficeScan 11.0 may unexpectedly block the transfer of files that contain personal names.

Solution: This hot fix enhances the Data Loss Prevention update program to ensure that OfficeScan 11.0 blocks files correctly under US Data Loss Prevention templates.

Hot Fix Build 1641.1

Issue 1: In OfficeScan 11.0, it may take a few minutes to save the Device Control/DLP settings on the OfficeScan web console when there is a large number of domains in the database.

Solution 1: This hot fix updates the OfficeScan 11.0 server and agent files to improve OfficeScan's performance in saving the Device Control/DLP settings on the OfficeScan web console.

Issue 2: OfficeScan 11.0 Patch 1 may not be able to recognize token variables in the "Subject" field of C&C callback notification email messages. As a result, the token names appear instead of the corresponding information.

Solution 2: This hot fix ensures that OfficeScan 11.0 Patch 1 recognizes token variables in the "Subject" field of C&C callback notification email messages and replaces these variables with the correct information.

Hot Fix Build 1643

Issue: When the OfficeScan client detects system events while the "EnableEventLog" option is enabled, the corresponding NT event logs do not appear in the Microsoft(TM) Windows(TM) event log file.

Solution: This hot fix ensures that when OfficeScan clients detect system events while the "EnableEventLog" option is enabled, the OfficeScan client NT event log function adds the corresponding NT event log to the Windows event log file.

Hot Fix Build 1768

Issue: Users cannot sort OfficeScan agents on the management tree by conventional scan pattern. This occurs because OfficeScan sorts the agents using the "VIRUS_PTN" field name instead of "PTNFILE" which is the correct field name for the conventional scan pattern information.

Solution: This hot fix enables OfficeScan to check the value of the "SORT_COLUMN" field so that if this is set to "VIRUS_PTN", OfficeScan will change it to "PTNFILE". This helps ensure that users can successfully sort OfficeScan agents on the management tree by conventional scan pattern.

Hot Fix Build 1799

Issue 1: A blank page appears when users attempt to access the Real-time Scan settings page on the OfficeScan web console.

Solution 1: This hot fix ensures that the Real-time Scan settings page on the OfficeScan web console displays properly.

Issue 2: The OfficeScan NT RealTime Scan service may cause the system to become unresponsive when running in conjunction with the Behavior Monitoring feature.

Solution 2: This hot fix updates the OfficeScan agent files which ensures that the Realtime Scan service does not cause the system to become unresponsive.

Issue 3: Some OfficeScan agents keep launching "upgrade.exe" because the OfficeScan server repeatedly sends several notifications for changes in the Scan Methods settings even when there are no changes.

Solution 3: This hot fix updates the OfficeScan server program to ensure that it sends the correct notifications to OfficeScan agents.

Hot Fix Build 1809

Issue 1: The OfficeScan Smart Protection Server (SPS) does not clean old shared memory information when the information changes. As a result, the SPS may not be able to retrieve the correct shared memory information when the computer starts after shutting down unexpectedly.

Solution 1: This hot fix enables the SPS to automatically clean old shared memory information each time the information changes.

Issue 2: When a pattern update fails, the SPS module does not delete the new pattern files from the "activeupdate" folder. If for some reason, pattern updates fail multiple times, successively, the "activeupdate" folder will grown and take up more disk space.

Solution 2: This hot fix enables the SPS to promptly delete new pattern files from the "activeupdate" folder when a pattern update fails. This hot fix also improves the pattern update mechanism to help ensure that patterns are updated successfully.

Hot Fix Build 1811

Issue 1: Before an OfficeScan agent runs an on-demand scan, it first checks the on-demand scan cache for files to exclude from the scan to reduce scanning time. Sometimes, on-demand scans take a long time to complete because some files may be scanned redundantly when the on-demand scan cache does not work properly.

Solution 1: This hot fix prevents this performance issue by updating the OfficeScan server and agent files.

Issue 2: The information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan (Scan Now)" fields on the "Agent Management" page of the OfficeScan web console are not updated after a Manual Scan or a Scan Now task completes.

Solution 2: This hot fix updates some OfficeScan files to ensure that the information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan (Scan Now)" fields on the "Agent Management" page of the OfficeScan web console are updated promptly after each virus scan task.

Hot Fix Build 1812

Issue: Gmail, Google Drive, and other Google-supported web sites have switched to the HTTP2 networking protocol but the Trend Micro Data Loss Prevention(TM) 6.0 agent cannot detect HTTP2 violations.

Solution: This hot fix enables OfficeScan client Data Loss Prevention Endpoints to monitor HTTP2 activity.

Hot Fix Build 1813

Issue: An issue prevents users from saving changes to the scan trigger settings of Real-time Scan on the OfficeScan client console.

Solution: This hot fix ensures that users can successfully edit and save changes in the scan trigger settings of Real-time Scan on the OfficeScan client console.

Hot Fix Build 1824

Issue: When the OfficeScan client detects system events while the "EnableEventLog" option is enabled, the corresponding NT event logs do not appear in the Microsoft(TM) Windows(TM) event log file.

Solution: This hot fix ensures that when OfficeScan clients detect system events while the "EnableEventLog" option is enabled, the OfficeScan client NT event log function adds the corresponding NT event log to the Windows event log File.

Hot Fix Build 1827

Issue: After enabling Data Loss Prevention, copying files from a network location to an FTP location causes users to disconnect from the network due to insufficient access privileges.

Solution: This hot fix resolves the Remote Desktop Protocol (RDP) disconnection issue when copying files from SMB. This hot fix also verifies the privileges on the endpoint before copying files to prevent the endpoint from hanging when the copy process begins.

Hot Fix Build 1828

Enhancement: This hot fix extends the email domain exceptions size to 40960 for monitored and non-monitored email domains of Email clients in Data Loss Prevention policy settings.

Hot Fix Build 1829

Issue: An incompatibility issue between the OfficeScan Advanced Protection Service and Microsoft(TM) Internet Explorer(TM) can prevent users from downloading and viewing .xdw files in the browser.

Solution: This hot fix ensures that the OfficeScan Advanced Protection Service works well with Internet Explorer.

Hot Fix Build 1829.1

Issue: Sometimes, the Trend Micro TDI (TMTDI) driver which provides network traffic monitoring for the Web Reputation Server of OfficeScan agents may trigger performance issues on computers running on Microsoft(TM) Windows(TM) Server platforms.

Solution: This hot fix allows users to uninstall the TMTDI driver globally from all OfficeScan agents installed on any Windows Server platform.

Hot Fix Build 1833

Issue: Some compressed OfficeScan agent files cannot be extracted successfully preventing users from opening the OfficeScan agent console.

Solution: This hot fix updates some OfficeScan files to ensure that compressed agent files can be extracted properly and the OfficeScan agent console opens normally.

Hot Fix Build 1835

Issue: When an OfficeScan server uses an SQL Server as a database, the "DbServer.exe" process encounters a database exception error and stops unexpectedly, if it encounters a null value in the agent domain information.

Solution: This hot fix updates the SQL procedure in the OfficeScan server program to enable "DbServer.exe" to handle null values properly.

Hot Fix Build 1836

Enhancement: This hot fix enables users to configure a Web Reputation policy for agents running Microsoft(TM) Windows(TM) Server 2003, Windows Server 2008, or Windows Server 2012 by selecting the root domain icon, specific domains, or specific agents in the "Agent Management" page of the OfficeScan web console.

Hot Fix Build 1837

Issue: When Trend Micro Data Loss Prevention(TM) upgrades from version 5.7 to 6.0, the upgrade program does not stop the OfficeScan Data Protection Service which prevents it from overwriting some files. This causes the update to fail with some files successfully updated to version 6.0 while the rest remain in version 5.7. Under this scenario, blue screen of death (BSOD) occurs while the Data Loss Prevention agent applies the settings to the driver.

Solution: This hot fix enhances the Data Loss Prevention update program to ensure that it stops the OfficeScan Data Protection Service before running the upgrade.

Hot Fix Build 1838

Issue: Sometimes, an issue with the exclusive control logic in the TmPfw and TmWfp filters may trigger both to register the TmWfp filter driver at the same time.

Solution: This hot fix updates the Network Security Components to ensure that the TmWfp filter driver can only be registered to either the TmPfw or TmWfp filter and not to both at the same time.

Hot Fix Build 1839

Issue 1: When the OfficeScan server handles large C&C Callback logs for outbreak email notifications, the OfficeScan Master Service may stop responding.

Solution 1: This hot fix updates OfficeScan server files to handle large C&C Callback logs for outbreak email notifications successfully.

Issue 2: The email content for C&C Callbacks outbreak email notifications has incorrect information.

Solution 2: This hot fix updates OfficeScan server files to provide correct information for C&C Callback outbreak email notifications.

Issue 3: A stored procedure uses a string that contains a list of UIDs separated by commas as its first parameter. If the string is longer than 4 KB and the stored procedure is used to query a UID table column, the MSSQL server returns an exception.

Solution 3: This hot fix prevents the SQL error from occurring in the scenario described above.

Hot Fix Build 1840

Issue: The Trend Micro Data Loss Prevention(TM) module of OfficeScan 11.0 does not support Microsoft(TM) Windows(TM) To Go 8.1.

Solution: This hot fix updates the Data Loss Prevention module in OfficeScan 11.0 to support Windows To Go 8.1.

Hot Fix Build 1844

Issue: Blue screen of death (BSOD) may occur on endpoints running Microsoft(TM) Windows(TM) 10 and protected by both Trend Micro OfficeScan(TM) and Lumension Security(TM) software.

Solution: This hot fix resolves the compatibility issue between the OfficeScan client program and Lumension Security to prevent the BSOD issue on protected endpoints.

Hot Fix Build 1845

Enhancement: This hot fix updates the OfficeScan agent program and Virus Scan Engines to enhance the Files Self Protection function in OfficeScan agents.

This enhancement requires users to deploy the new Virus Scan Engines to agents. The steps are included in the installation procedure.

Hot Fix Build 1846

Issue: In the Spyware/Grayware log screen, users encounter a "SyntaxError: Invalid Character" message after selecting a spyware record and clicking the "Add to approved list" link. When this happens, garbled characters appear in the domain information field on the page.

Solution: This hot fix ensures that users can add spyware records into the approved list without issues and that the correct domain information appears without garbage characters in the Spyware/Grayware log screen.

Hot Fix Build 1847

Enhancement: This hot fix included the following enhancement: 1. Support Diners Club credit card number in the "CreditCardNumber" validator.

Hot Fix Build 1851

Issue: After deploying policy settings from the Control Manager server to OfficeScan agents, only one agent applies the updated settings when the OfficeScan server uses a SQL database.

Solution: After applying this hotfix, all targeted OfficeScan agents successfully apply the settings sent from the Control Manager server.

Hot Fix Build 1853

Enhancement: This hotfix included the following enhancement for Trend Micro Data Loss Prevention(TM) module in OfficeScan 11.0. 1. American Name validator is not case sensitive.

Hot Fix Build 1855

Issue: OfficeScan's list of approved spyware and grayware contains the names of files and applications that users do not want OfficeScan to treat as spyware or grayware, however, OfficeScan may keep treating a particular file or application on the list as spyware or grayware.

Solution: This hot fix updates the OfficeScan server and agent programs to ensure that OfficeScan does not treat any file or application on the approved list as spyware or grayware.

Hot Fix Build 1857

Issue: When users export the list of agents and select multiple domains, the exported file will not contain any information.

Solution: This hot fix ensures that users can successfully export the list of agents when multiple domains are selected.

Hot Fix Build 1863

Issue: On the OfficeScan agent console, Scan Operation Logs display an end time even when the status of a scan is "Stopped Unexpectedly".

Solution: This hot fix updates the OfficeScan agent program to allow Scan Operation Logs to display "N/A" in the end time field if the scan status is "Stopped Unexpectedly".

Hot Fix Build 1865

Issue: OfficeScan 11.0 allows administrators to migrate the existing OfficeScan database from its native CodeBase to an SQL server database. For some reason, when OfficeScan uses an SQL server, users cannot save the scan exclusion settings on the "Scanning settings" page of the OfficeScan web console.

Solution: This hot fix updates the OfficeScan server program to ensure that users can save the scan exclusion settings when OfficeScan uses an SQL database.

Hot Fix Build 1865 replaced by Hot Fix Build 1912

Issue 1: Sometimes, the agent program version is not updated promptly after users apply a hot fix on the OfficeScan server and the new agent-side programs have been successfully deployed to agent computers.

Solution 1: This hot fix updates the OfficeScan server and agent programs to ensure that OfficeScan agents update the program version information promptly after applying updates from the OfficeScan server.

Issue 2: In environments where Remote Desktop Protocol (RDP) or Independent Computing Architecture (ICA) is used to connect to a Citrix(TM) terminal server, users may encounter an issue with the OfficeScan agent's Trend Micro Data Loss Prevention(TM) (DLP) add-in that may cause Microsoft(TM) Outlook(TM) to stop responding.

Solution 2: This hot fix updates OfficeScan agent programs which resolve this issue on RDP or ICA connections on the Citrix terminal server environment.

Hot Fix Build 1874

Issue: In computers protected by Data Loss Prevention (DLP) of OfficeScan agent, when the device control function for "wireless adapter" is enabled, DLP also blocks the "USB LAN adapter".

Solution: This hot fix ensures that DLP of OfficeScan agent does not block the "USB LAN adapter" when the device control function for "wireless adapter" is enabled.

Hot Fix Build 1876

Issue: Sometimes, an issue with the exclusive control logic in the TmPfw and TmWfp filters may trigger both to register the TmWfp filter driver at the same time.

Solution: This hot fix updates the Network Security Components to ensure that the TmWfp filter driver can only be registered to either the TmPfw or TmWfp filter and not to both at the same time.

Hot Fix Build 1876.1

Issue: Sometimes, when OfficeScan is integrated with an Active Directory (AD) that contains a large number of organizational units (OU), the total number of agents indicated on the OfficeScan Unmanaged Endpoints Assessment page does not match the number of agents in the AD.

Solution: This hot fix resolves this issue by ensuring that the OfficeScan server can successfully retrieve information on all computers under the user-defined AD scope while running Unmanaged Endpoints assessment.

Hot Fix Build 1886 replaced by Hot Fix Build 1912

Issue: When users delete organizational units (OU) from the Active Directory (AD), the OUs remain in the "Custom agent groups" list of OfficeScan domains even when the OUs do not contain any OfficeScan agent.

Solution: This hot fix enables OfficeScan to determine if a deleted AD OU contains any OfficeScan agent, and to delete these from the "Custom agent groups" list if these do not contain any Officescan agent.

Hot Fix Build 1902

Issue: OfficeScan servers do not send out an SQL Database Unavailable Alert when the SQL connection fails.

Solution: This hot fix ensures that the OfficeScan server sends an SQL Database Unavailable Alert when the SQL connection fails.

Hot Fix Build 1906

Enhancement: This hot fix enables OfficeScan to save the last setting for the number of user accounts that can be displayed in a single page on the OfficeScan web console "Administration > Account Management > User Accounts" page. As a result, the OfficeScan web console will display the same number of user accounts on the page after users leave and then return to the page.

Hot Fix Build 1912

Issue 1: An issue prevents users from saving changes to the scan trigger settings of Real-time Scan on the OfficeScan client console.

Solution 1: This hot fix ensures that users can successfully edit and save changes in the scan trigger settings of Real-time Scan on the OfficeScan client console.

Issue 2: When users delete organizational units (OU) from the Active Directory (AD), the OUs remain in the "Custom agent groups" list of OfficeScan domains even when the OUs do not contain any OfficeScan agent.

Solution 2: This hot fix enables OfficeScan to determine if a deleted AD OU contains any OfficeScan agent, and to delete these from the "Custom agent groups" list if these do not contain any Officescan agent.

Issue 3: Sometimes, the agent program version is not updated promptly after users apply a hot fix on the OfficeScan server and the new agent-side programs have been successfully deployed to agent computers.

Solution 3: This hot fix updates the OfficeScan server and agent programs to ensure that OfficeScan agents update the program version information promptly after applying updates from the OfficeScan server.

Issue 4: In environments where Remote Desktop Protocol (RDP) or Independent Computing Architecture (ICA) is used to connect to a Citrix(TM) terminal server, users may encounter an

issue with the OfficeScan agent's Trend Micro Data Loss Prevention(TM) (DLP) add-in that may cause Microsoft(TM) Outlook(TM) to stop responding.

Solution 4: This hot fix updates OfficeScan agent programs which resolve this issue on RDP or ICA connections on the Citrix terminal server environment.

Hot Fix Build 1913

Issue: Sometimes the Trend Micro Active Update module does not delete unnecessary update folders from the "OfficeScan installation path¥Web¥Service¥AU_Data¥AU_Storage" folder.

Solution: This hot fix updates the Trend Micro Active Update module to ensure that it deletes unnecessary update folders from the "OfficeScan installation path¥Web¥Service¥AU_Data¥ AU_Storage" folder.

The unnecessary folder delete action will be trigger in next successful update event. After the HF installation, please hold on until next OfficeScan server update.

Hot Fix Build 1914

Issue: The OfficeScan client cannot successful perform a manual scan on a remote drive that runs on a Microsoft(TM) Windows(TM) XP platform.

Solution: This hot fix ensures that the OfficeScan client successful performs a manual scan on a Microsoft Windows XP remote drive.

Hot Fix Build 1915

Issue 1: Under certain conditions, the Trend Micro Data Loss Prevention(TM) (DLP) module of OfficeScan may stop responding while opening a new connection because the DLP agent stops unexpectedly.

Solution 1: This hot fix ensures that the DLP module of OfficeScan can successfully open a new connection.

Issue 2: The DLP module of OfficeScan does not block users from sending out a new email message on Gmail when two of its file attachments have the same name but are saved in different folders.

Solution 2: This hot fix ensures that DLP of OfficeScan can block users from sending out this type of email messages.

Issue 3: OfficeScan cannot block users from uploading sensitive files to Gmail in Mozilla(TM) Firefox(TM) version 38 or Chorme(TM) version 43.

Solution 2: This hot fix ensures that OfficeScan can effectively block users from uploading sensitive files to Gmail.

Hot Fix Build 1916

Issue 1: Sometimes, the Microsoft(TM) Windows(TM) event viewer log reports that a deadlock error occurred in the OfficeScan SQL server.

Solution 1: This hot fix prevents the deadlock issue in the OfficeScan SQL server.

Issue 2: The OfficeScan agent cannot report its IP address to the server when the computer is connected through a mobile network, for example, an 4G LTE network.

Solution 2: This hot fix updates the OfficeScan agent program to ensure that it can report its IP address to the OfficeScan server when the computer is connected through a mobile network.

Hot Fix Build 1916

Issue: The OfficeScan Master Service, "OfcService.exe", stops unexpectedly while managing OfficeScan tasks.

Solution: This hot fix updates the OfficeScan server files to resolve this issue.

Enhancement: This hot fix enables the OfficeScan 11.0 server to download the list of approved USB devices of the Device Control Settings from the Trend Micro Control Manager(TM) server and to deploy the list to OfficeScan agents.

The list of approved USB devices supports up to 18,000 devices.

Hot Fix Build 1919

Issue: OfficeScan clients show corrupt firewall profile information after upgrading from OfficeScan 10.5 or the previous versions.

Solution: This hot fix ensures that the OfficeScan client checks the size of the firewall profile and uses the correct method of parsing firewall profiles after an OfficeScan client upgrade.

Hot Fix Build 1920

Issue: The Trend Micro Behavior Monitoring feature may trigger a performance issue in Visio Studio +Qt.

Solution: This hot fix ensures that the Trend Micro Behavior Monitoring feature works well with the Visio Studio +Qt.

Hot Fix Build 1921

Issue: The following error message appears when users click on the client count link on the dashboard search page of the OfficeScan web console:

"An error occurred. Make sure your network connection is active and that the OfficeScan service is running. If you encounter this error again, contact your support provider for troubleshooting assistance."

Solution: This hot fix extends the cache size for the OfficeScan web console so users can successfully view the client count information after clicking on the link on the dashboard search page without triggering the error message.

Hot Fix Build 1924

Issue 1: The Trend Micro Data Loss Prevention(TM)(DLP) module in OfficeScan 11.0 triggers version 43 of the x64 Google Chrome(TM) web browser to stop unexpectedly.

Solution 1: This hot fix updates the DLP module to resolve the issue.

Issue 2: An issue with the DLP module in OfficeScan 11.0 can cause some inconsistent information to appear in violation logs.

Solution 2: This hot fix updates the DLP module to ensure that OfficeScan violation log contain the correct information.

Hot Fix Build 1929

Enhancement: This hot fix enables the Trend Micro Data Loss Prevention(TM) (DLP) module in OfficeScan 11.0 Patch 1 to check an email message's transmission scope using the domain information of email recipients. Users can also configure the DLP module to treat

either gmail.com or Trend Micro Taiwan as internal domains and to skip the checking if the policy is set to check WAN traffic only.

Hot Fix Build 1933

Issue: On x64 platforms, the way Trend Micro Behavior Monitor Service processes an information entry may cause the system to become unresponsive.

Solution: This hot fix updates the common module for Trend Micro Behavior Monitor Service to resolve this issue.

Hot Fix Build 1934

Enhancement: This hot fix ensures that OfficeScan displays Trend Micro Data Loss Prevention(TM) violation notification pop ups in the correct session by enabling it to check if the user name in the pop up window matches the login name for the current session before displaying the pop up.

Hot Fix Build 1941

Issue 1: A large number of old files accumulate in the "OfficeScan installation path¥Web¥Service¥AU_Data¥ AU_Storage" folder when the ActiveUpdate module encounters a merge error.

Solution 1: This hot fix updates the ActiveUpdate module to ensure that it deletes unnecessary update folders from the "OfficeScan installation path¥Web¥Service¥AU_Data¥ AU_Storage" folder.

Issue 2: The OfficeScan server cannot download components from the Trend Micro Control Manager(TM) server through the SSL protocol using the Control Manager's IPv6 address.

Solution 2: This hot fix updates the ActiveUpdate module to ensure that it can connect to the Control Manager server using the SSL protocol using the Control Manager's IPv6 address.

Hot Fix Build 1944

Issue: When CGI applications become unresponsive due to multiple agent requests in the queue, the OfficeScan server master service stops accepting new requests from agents.

Solution: This hot fix updates the master service module to resolve this issue.

Hot Fix Build 1946

Issue: When the OfficeScan client detects system events while the "EnableEventLog" option is enabled, the corresponding NT event logs do not appear in the Microsoft(TM) Windows(TM) event log file.

Solution: This hot fix ensures that when OfficeScan clients detect system events while the "EnableEventLog" option is enabled, the OfficeScan client NT event log function adds the corresponding NT event log to the Windows event log file.

Hot Fix Build 1948

Issue: Blue screen of death (BSOD) may occur when the Tmeext driver encounters a NULL pointer value.

Solution: This hot fix adds an error-handling mechanism to the Tmeext driver to enable it to handle NULL pointer values.

Hot Fix Build 1949

Issue: Sometimes, the File Reputation Service information disappears from the Management Console even when the service is active on the OfficeScan agent and old pattern files remain in the agent folder after a new version has been downloaded successfully.

Solution: This hot fix resolves the issues by updating the Trend Micro iCRC common module.

Hot Fix Build 1950

Issue: Sometimes, an OfficeScan agent encounters performance issues when its Damage Cleanup Services (DCS) (TSC.exe) checks the digital signature of files and the Microsoft(TM) Windows(TM) certificate on the agent computer is outdated.

Solution: This hot fix allows users to prevent DCS from checking digital signatures.

Hot Fix Build 1951

Issue: A third-party Java(TM) application may stop responding when the Web Reputation feature is enabled on computers protected by OfficeScan 11.

Solution: This hot fix ensures that the third-party Java application works normally on protected computers.

Hot Fix Build 1952

Enhancement: This hot fix enables Trend Micro Data Loss Prevention(TM) (DLP) Endpoint SDK 6.0 to support up to the BETA version 44.0.2403.61 of the 32 and 64-bit Google Chrome web browser.

Hot Fix Build 1957

Issue: The wrong firewall status may appear for some OfficeScan agents on the "Agent Management" page of the OfficeScan web console.

Solution: This hot fix ensures that the correct OfficeScan agent firewall status appears on the "Agent Management" page of the OfficeScan web console.

Hot Fix Build 1959

Issue: When multiple OfficeScan agents register to the OfficeScan server with the agent grouping rule enabled, the GenerateSAF process may prevent new OfficeScan agents from registering to the OfficeScan server.

Solution: This hot fix resolves this issue so that new OfficeScan agents can register to the OfficeScan server successfully.

Hot Fix Build 1960

Issue: Users encounter a 502 error while attempting to export the list of OfficeScan agents on the root domain through the OfficeScan web console.

Solution: This hot fix ensures that users can successfully export the list of OficeScan agents on the root domain.

Hot Fix Build 1966

Issue 1: When the OfficeScan agent has just restarted or when users access the Google Drive in Google Chrome(TM) for the first time, users may be able to drag and drop sensitive files to the Google Drive.

Solution 1: This hot fix updates the Trend Micro Data Loss Prevention(TM) (DLP) module in OfficeScan 11.0 to ensure that users will not be able to drag and drop sensitive files to Google Drive.

Issue 2: Users receive a violation alert while attempting to access Facebook(TM) if Skype(TM) Click To Call(TM) is enabled.

Solution 2: This hot fix updates the DLP module to ensure that users do not receive a violation alert under the scenario described above.

Hot Fix Build 1967

Issue: When an OfficeScan server detects that an OfficeScan client program file cannot run because of an invalid certificate, it renames the file by adding the "_invalid" suffix. Sometimes, the OfficeScan server cannot rename these program files which may allow the server to delete these files by mistake.

Solution: This hot fix ensures that the OfficeScan server does not delete OfficeScan client program files that it cannot rename.

Hot Fix Build 1968

Issue: The OfficeScan web console is affected by a cross-site scripting (XSS) vulnerability.

Solution: This hot fix updates the OfficeScan web console program to resolve the vulnerability.

Hot Fix Build 1971

Issue: Domain names that contain garbled characters cannot be displayed correctly in the client tree on the OfficeScan web console.

Solution: This hot fix provides an option to allow users to filter a predefined special keyword such as a special character for the sorting rule. This helps ensure that the OfficeScan server can successfully display domain names in the client tree using Automatic Agent Grouping.

Hot Fix Build 1972

Issue 1: OfficeScan uses public-key cryptography to authenticate communications that the OfficeScan server initiates on agents. The OfficeScan server Master Service may stop responding when using an invalid public key certificate.

Solution 1: This hot fix enhances the certificate management of OfficeScan to prevent the OfficeScan Master Service from becoming unresponsive.

Issue 2: The name of and paths to infected files cannot be displayed correctly in outbreak email notifications from OfficeScan.

Solution 2: This hot fix updates the OfficeScan server files to ensure that outbreak email notifications always contain and display complete and accurate information.

Hot Fix Build 1974

Issue: Sometimes, the Trend Micro iCRC common module encounters a memory leak issue.

Solution: This hot fix updates the Trend Micro iCRC common module to resolve the memory leak issue.

Hot Fix Build 1974.1

Issue: The OfficeScan web console may not be able to display the correct scan exclusion settings of some OfficeScan clients. This occurs because OfficeScan clients cannot upload the settings successfully if the settings contain an "%" character.

Solution: This hot fix enables OfficeScan clients to upload the scan exclusion settings successfully which ensures that the Officescan web console displays the correct scan exclusion settings of OfficeScan clients.

Hot Fix Build 1975

Issue: The OfficeScan server cannot apply the firewall policy to an OfficeScan client if the client's IP address is retrieved using certain VPN client programs.

Solution: This hot fix updates the OfficeScan server and client programs to ensure that the OfficeScan server can successfully apply the firewall policy to clients.

JP Hot Fix Build 1977

Issue: On the OfficeScan agent console, Scan Operation Logs display an end time even when the status of a scan is "Stopped Unexpectedly".

Solution: This hot fix updates the OfficeScan agent program to allow Scan Operation Logs to display "N/A" in the end time field if the scan status is "Stopped Unexpectedly".

Hot Fix Build 1979

Enhancement: This hot fix enables the OfficeScan 11.0 server to download the list of approved USB devices of the Device Control Settings from the Trend Micro Control Manager(TM) server and to deploy the list to OfficeScan agents.

The list of approved USB devices supports up to 18,000 devices.

Hot Fix Build 1980

Issue: Users cannot create a file exclusion list for manual and scheduled scans from the OfficeScan client console.

Solution: This hot fix enables users to create a file exclusion list for manual and scheduled scans from the OfficeScan client console.

Hot Fix Build 1981

Issue: The Trend Micro Data Loss Prevention(TM) (DLP) module supports the single asterisk wild card character (*) in its file attribute list but the OfficeScan web console does not accept this. For example, the DLP module accepts the following file attribute list but the OfficeScan web console does not allow it: - *.

Solution: This hot fix enables the OfficeScan web console to allow users to use a single asterisk wild card character in the DLP file attribute list.

Hot Fix Build 1985

Enhancement: This hot fix enables users to generate the Secure Sockets Layer (SSL) certificate with 2048-bit public key for the OfficeScan web site which is installed on Microsoft(TM) Internet Information Services (IIS) through the SvrSvcSetup.exe tool.

Hot Fix Build 1987

Issue: The OfficeScan agent PccNT process stops unexpectedly and triggers an access violation event once or twice a week.

Solution: This hot fix prevents the OfficeScan Agent PccNT process from stopping unexpectedly.

Hot Fix Build 1990

Issue: JP version installer displayed English wording.

Solution:

This hot fix the displayed.

Hot Fix Build 1995

Issue: While running a scan, the OfficeScan agent may unexpectedly launch the "TSCCensus.exe" process which is used for Smart Protection Network feedback. When this happens on the Microsoft(TM) Windows(TM) platform, Windows opens a command prompt to "C:¥WINDOWS¥ TSCCensus.exe".

Solution: This hot fix allows users to prevent "TSCCensus.exe" from running while the OfficeScan agent is running a scan.

Hot Fix Build 1995

Issue: The "days" setting in the "Privileges and Other Settings > Cache Settings for Scans" page of the OfficeScan web console automatically resets to "0" after the server deploys the other settings to OfficeScan agents.

Solution: This hot fix updates the OfficeScan 11.0 Service Pack 1 server and agent files to resolve this issue.

Hot Fix Build 1997

Issue: A mismatch between the encode and decode calling mechanism prevents OfficeScan from syncing up with the Active Directory server.

Solution: This hot fix resolves the call mismatch issue so OfficeScan can sync up with the Active Directory server successfully.

Hot Fix Build 1998

Issue: Temp files that DLP module is using fill up disk space.

Solution: This hot fix resolves the disk space usage issue.

Hot Fix Build 2003

Issue: Users may encounter the "Unknown error. Please try again." message when saving changes to the Real-time Scan Settings of a particular domain. This occurs when OfficeScan attempts to convert an empty string.

Solution: This hot fix updates the OfficeScan 11.0 server and agent files so users can successfully edit and save the Real-time Scan Settings for domains.

Hot Fix Build 2005

Issue 1: When the OfficeScan agent has just restarted or when users access the Google Drive in Google Chrome(TM) for the first time, users may be able to drag and drop sensitive files to the Google Drive.

Solution 1: This hot fix updates the Trend Micro Data Loss Prevention(TM) (DLP) module in OfficeScan 11.0 to ensure that users will not be able to drag and drop sensitive files to Google Drive.

Issue 2: Users receive a violation alert while attempting to access Facebook(TM) if Skype(TM) Click To Call(TM) is enabled.

Solution 2: This hot fix updates the DLP module to ensure that users do not receive a violation alert under the scenario described above.

Hot Fix Build 2006

Issue: OfficeScan clients that are installed on Microsoft(TM) Windows(TM) Server 2012 R2 with Domain Controller are displayed as "WindowsNT Platform Series" on the agent management tree. This happens because the Window API uses a stand-alone type to indicate the domain controller server and some OfficeScan server programs cannot handle this type.

Solution: This hot fix enables OfficeScan to handle domain controller server types so it can display the correct information on the agent management tree.

Hot Fix Build 2007

Issue: An issue may interrupt the remote desktop connection in an OfficeScan 11.0 agent computer which triggers the Real-Time Scan service to stop unexpectedly.

Solution: This hot fix updates the OfficeScan server and client files to resolve this issue.

Hot Fix Build 2015

Issue: When users hide a drive through a group policy, the drive will still be visible in the folder tree on the manual scan page of the OfficeScan 11 agent console.

Solution: This hot fix ensures that the OfficeScan agent displays only the applicable drives in the folder tree on the manual scan page.

Hot Fix Build 2017

Enhancement: Currently, when an OfficeScan server applies a Trend Micro Data Loss Prevention(TM) hot fix, it notifies all managed OfficeScan clients to apply the update. This hot fix allows users to configure certain OfficeScan clients so that these clients do not automatically apply Data Loss Prevention updates from the OfficeScan server.

Hot Fix Build 2018

Issue: The AEGIS module of the OfficeScan 11.0 agent program may trigger some processes to close unexpectedly.

Solution: This hot fix updates the Behavior Monitoring Service module in OfficeScan 11.0 to ensure that the AEGIS module no longer triggers processes to close unexpectedly.

Hot Fix Build 2020

Enhancement: This hot fix enables Data Loss Prevention Endpoint SDK 6.0 to support up to version 46.0.2490.80 of the 32 and 64-bit Google Chrome(TM) web browser.

Hot Fix Build 2023

Issue: It may take a long time to log on to computers protected by OfficeScan 11.0 when the Browser Exploit Prevention feature is enabled.

Solution: This hot fix updates the Browser Exploit Prevention module in OfficeScan 11.0 to ensure that users can log on to protected computers without issues.

Hot Fix Build 2024

Enhancement: This hot fix enables the Trend Micro Data Loss Prevention(TM) module in OfficeScan 11.0 to support the following:

- version 43.0.3 of the 32 and 64-bit Mozilla(TM) Firefox(TM) web browser
- up to version 47.0.2526.106 of the 32 and 64-bit Google Chrome(TM) web browser

Hot Fix Build 2030

Issue: An issue with the way OfficeScan handles scan threads may prevent users from transferring OfficeScan agents between OfficeScan servers, trigger an OfficeScan server to stop responding, or cause the NT RealTime Scan service to stop unexpectedly.

Solution: This hot fix updates the OfficeScan server and client files to resolve the scan thread handling issue.

Hot Fix Build 2042

Issue: The OfficeScan agent program may be vulnerable to potential unintended file access attacks.

Solution: This hotfix improves a checking mechanism in the OfficeScan agent program to protect it against unintended file access attacks.

Hot Fix Build 2044

Issue: The TMEBC driver does not start during the system boot process because the TMEBC driver file (TMEBC32.SYS on 32-bit platforms or TMEBC64.SYS on 64-bit platforms) is not in the C:¥Windows¥system32¥DRIVERS directory while the corresponding registry entry still exists on the Services screen.

Solution: This hotfix resolves this issue by installing the TMEBC driver on OfficeScan agents if the TMEBC driver is not installed or if the TMEBC driver file is missing.

Issues resolved by hot fixes for OSCE 11.0 SP1

Hot Fix Build 2998

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 3010

Issue: After deploying policy settings from the Control Manager server to OfficeScan agents, only one agent applies the updated settings when the OfficeScan server uses a SQL database.

Solution: After applying this hotfix, all targeted OfficeScan agents successfully apply the settings sent from the Control Manager server.

Hot Fix Build 3013

Issue: In environments where Remote Desktop Protocol (RDP) or Independent Computing Architecture (ICA) is used to connect to a Citrix(TM) terminal server, users may encounter an issue with the OfficeScan agent's Trend Micro Data Loss Prevention(TM) (DLP) add-in that may cause Microsoft(TM) Outlook(TM) to stop responding.

Solution: This hot fix updates OfficeScan agent programs which resolve this issue on RDP or ICA connections on the Citrix terminal server environment.

Hot Fix Build 3014

Issue: In computers protected by Data Loss Prevention (DLP) of OfficeScan agent, when the device control function for "wireless adapter" is enabled, DLP also blocks the "USB LAN adapter".

Solution: This hot fix ensures that DLP of OfficeScan agent does not block the "USB LAN adapter" when the device control function for "wireless adapter" is enabled.

Hot Fix Build 3014.1

Issue: OfficeScan 11.0 service pack 1 may not be able to recognize token variables in the "Subject" field of C&C callback notification email messages. As a result, the token names appear instead of the corresponding information.

Solution: This hot fix ensures that OfficeScan 11.0 service pack 1 recognizes token variables in the "Subject" field of C&C callback notification email messages and replaces these variables with the correct information.

Hot Fix Build 3015 merged from Hot Fix Build 1635

Issue 1: Before an OfficeScan agent runs an on-demand scan, it first checks the on-demand scan cache for files to exclude from the scan to reduce scanning time. Sometimes, on-demand scans take a long time to complete because some files may be scanned redundantly when the on-demand scan cache does not work properly.

Solution 1: This hot fix prevents this performance issue by updating the OfficeScan server and agent files.

Issue 2: Users that do not have administrator privileges still have full access to the OfficeScan client program directory after users switch the OfficeScan client's security setting from "Normal" to "High".

Solution 2: This hot fix ensures that the OfficeScan client program automatically limits users that do not have administrator privileges to read-only access to the OfficeScan client program directory when the security setting is switched to "High".

Hot Fix Build 3016

Issue: When users trigger the "Scan Now" feature of an OfficeScan agent to run a manual scan, some drives do not appear in the scan folder selection box.

Solution: This hot fix updates some OfficeScan files to ensure that the scan folder selection box displays all drives under the scenario described above.

Hot Fix Build 3017

Issue: Sometimes, an issue with the exclusive control logic in the TmPfw and TmWfp filters may trigger both to register the TmWfp filter driver at the same time.

Solution: This hot fix updates the Network Security Components to ensure that the TmWfp filter driver can only be registered to either the TmPfw or TmWfp filter and not to both at the same time.

Hot Fix Build 3018 merged from Hot Fix Build 1799

Issue 1: The OfficeScan NT RealTime Scan service may cause the system to become unresponsive when running in conjunction with the Behavior Monitoring feature.

Solution 1: This hot fix updates the OfficeScan agent files which ensures that the Realtime Scan service does not cause the system to become unresponsive.

Issue 2: Some OfficeScan agents keep launching "upgrade.exe" because the OfficeScan server repeatedly sends several notifications for changes in the Scan Methods settings even when there are no changes.

Solution 2: This hot fix updates the OfficeScan server program to ensure that it sends the correct notifications to OfficeScan agents.

Hot Fix Build 3019

Issue: OfficeScan servers do not send out an SQL Database Unavailable Alert when the SQL connection fails.

Solution: This hot fix ensures that the OfficeScan server sends an SQL Database Unavailable Alert when the SQL connection fails.

Hot Fix Build 3027

Enhancement: This hot fix enables users to configure a Web Reputation policy for agents running Microsoft(TM) Windows(TM) Server 2003, Windows Server 2008, or Windows Server 2012 by selecting the root domain icon, specific domains, or specific agents in the "Agent Management" page of the OfficeScan web console.

Hot Fix Build 3028

Issue: When the file input/output (I/O) task is intercepted by other applications, the OfficeScan agent Real-time Scan will not be able to perform the scan task and no error message is triggered.

Solution: This hot fix enables OfficeScan agents to check and display the progress of real-time scans on both the agent and server sides.

Hot Fix Build 3029

Enhancement: This hot fix allows users to configure the cache size for the OfficeScan web console to prevent certain issues such as a delayed response when users scroll left or right on

the OfficeScan web console when there is a large number of OfficeScan agents on a specific domain on the Agent Management tree.

Hot Fix Build 3030

Issue: When the scan operation file becomes corrupted for an unknown reason, it may cause the OfficeScan NT Listener service to crash during the OfficeScan agents upgrade.

Solution: This hot fix enables OfficeScan agents to check for invalid records in the scan operation log. If an invalid record is found, the OfficeScan agents will skip the invalid record and migrate to the next record.

Hot Fix Build 3036

Issue: In OfficeScan 11.0 Service Pack 1, it may take a few minutes to save the Device Control/DLP settings on the OfficeScan web console when there is a large number of domains in the database.

Solution: This hot fix updates the OfficeScan 11.0 Service Pack 1 server and agent files to improve OfficeScan's performance in saving the Device Control/DLP settings on the OfficeScan web console.

Hot Fix Build 3040

Issue: The TCacheGenCli tool does not respond to the "REMOVE_GUID" command.

Solution: This hot fix ensures that the TCacheGenCli tool responds normally to the "REMOVE_GUID" command.

Hot Fix Build 3041

Issue: When the OfficeScan server updates OfficeScan agent settings to the database, the server purges old information without verifying the GUIDs for agents. As a result, OfficeScan agents that do not have a previous GUID entry in the database revert to default settings.

Solution: This hot fix adds a GUID checking mechanism that enables the OfficeScan server to verify if a particular agent GUID exists in the agent table of the database before updating the agent information. If a GUID does not exist in the agent table, the OfficeScan server returns an error message and does not overwrite the agent settings.

Hot Fix Build 3043

Issue: An issue related to the Tmosprey driver in OfficeScan 11.0 Service Pack 1 may trigger the Tmlisten.exe service to stop unexpectedly.

Solution: This hot fix updates the Tmosprey driver in OfficeScan 11.0 Service Pack 1 to resolve the issue.

Hot Fix Build 3044

Issue: When users upgrade an OfficeScan 10.6 client that was installed using an MSI package to version 11 Service Pack 1 through the "Update Now" function, the value in the "DisplayVersion" registry key is not updated promptly. When this happens, users will not be able to establish a VPN connection trough the Juniper network from the OfficeScan client computer.

Solution: This hot fix updates the value of the "DisplayVersion" registry key to ensure that users can successfully establish VPN connections through the Juniper network on affected computers.

Hot Fix Build 3044.1

Issue: An issue related to the OfficeScan Browser Exploit Solution feature triggers Microsoft(TM) Internet Explorer(TM) 8 to stop unexpectedly when users open a Microsoft Word document using a web application.

Solution: This hot fix ensures that the OfficeScan Browser Exploit Solution feature works well with Internet Explorer 8.

Hot Fix Build 3045

Issue: After an OfficeScan client is upgraded from version 10.6 to version 11 Service Pack 1, "Service Pack 1" does not appear in the agent version information.

Solution: This hot fix ensures that OfficeScan clients display the correct version information.

Hot Fix Build 3046

Enhancement: This hot fix enables OfficeScan to save the last setting for the number of user accounts that can be displayed in a single page on the OfficeScan web console "Administration > Account Management > User Accounts" page. As a result, the OfficeScan web console will display the same number of user accounts on the page after users leave and then return to the page.

Hot Fix Build 3048

Issue: In OfficeScan 11.0 Service Pack 1, users cannot assign OfficeScan agents to a multilayered domain that has been pre-defined in the agent computer before agent installation.

Solution: This hot fix updates the OfficeScan 11.0 Service Pack 1 server and agent files to allow users to assign agents to pre-defined multilayer domains.

Hot Fix Build 3050

Issue: Trend Micro Common Client Soultion Framework Service may become unresponsive when there is an interoperability issue between SHA256 certificates and an underlying 3rd-party SSL library.

Solution: This hot fix updates the related modules to resolve this issue.

Hot Fix Build 3051

Issue: A large number of old files accumulate in the "OfficeScan installation path¥Web¥Service¥AU_Data¥ AU_Storage" folder when the ActiveUpdate module encounters a merge error.

Solution: This hot fix updates the ActiveUpdate module to ensure that it deletes unnecessary update folders from the "OfficeScan installation path¥Web¥Service¥AU_Data¥ AU_Storage" folder.

Hot Fix Build 3052

Issue 1: The Trend Micro Data Loss Prevention(TM) (DLP) module of the OfficeScan agent program cannot detect the transfer of sensitive information when the OfficeScan agent self-protection function is enabled.

Solution 1: This hot fix updates the OfficeScan agent program to ensure that the DLP module can successfully detect the transfer of sensitive information.

Issue 2: Sometimes, an OfficeScan agent encounters performance issues when its Damage Cleanup Services (DCS) (TSC.exe) checks the digital signature of files and the Microsoft(TM) Windows(TM) certificate on the agent computer is outdated.

Solution 2: This hot fix allows users to prevent DCS from checking digital signatures.

Hot Fix Build 3053

Issue: A third-party Java(TM) application may stop responding when the Web Reputation feature is enabled on computers protected by OfficeScan 11 Service Pack 1.

Solution: This hot fix ensures that the third-party Java application works normally on protected computers.

Hot Fix Build 3054

Issue: When an OfficeScan 11 Service Pack 1 agent is configured not to upload firewall logs, it may automatically start uploading these logs after restarting.

Solution: This hot fix ensures that OfficeScan agents upload firewall logs only when enabled to do so.

Hot Fix Build 3054.1

Issue: The OfficeScan database becomes corrupted after an OfficeScan agent uploads an OfficeScan Data Protection log that exceeds the log length limit.

Solution: This hot fix prevents the OfficeScan database from reading long Data Protection logs.

Hot Fix Build 3055

Issue: After users install an OfficeScan 11 Service Pack 1 agent, they may encounter a pop-up error message while running Autopcc.exe to update the agent files.

Solution: This hot fix ensures that Autopcc.exe can successfully update agent files.

Hot Fix Build 3057

Issue: The "7410001377365 My Number - Registered Corporation" keyword can be detected in samples on Trend Micro OfficeScan(TM) client computers but not on OfficeScan server computers.

Solution: This hot fix ensures that Data Loss Prevention (DLP) Endpoint SDK 6.0 can detect the "7410001377365 My Number - Registered Corporation" keyword in OfficeScan server and client computers.

Enhancement 1: This hot fix enables Data Loss Prevention Endpoint SDK 6.0 to support up to version 44.0.2403.125 of the 32 and 64-bit Google Chrome(TM) web browser.

Enhancement 2: This hot fix enables Data Loss Prevention Endpoint SDK 6.0 to support Microsoft(TM) Driver Signing for the following DLP drivers:

- Sakfile.sys
- Sakcd.sys
- Dlpnetfltr.sys

Enhancement 3: This hot fix enables the Data Loss Prevention Endpoint SDK 6.0 "ListDeviceInfo.exe" tool to detect SCSI External HDD devices.

Hot Fix Build 3062

Issue: When users delete organizational units (OU) from the Active Directory (AD), the OUs remain in the "Custom agent groups" list of OfficeScan domains even when the OUs do not contain any OfficeScan agent.

Solution: This hot fix enables OfficeScan to determine if a deleted AD OU contains any OfficeScan agent, and to delete these from the "Custom agent groups" list if these do not contain any Officescan agent.

Hot Fix Build 3062.1

Issue: The Trend Micro Data Loss Prevention(TM) Endpoint SDK 6.0 module of the OfficeScan 11.0 agent program does not support the following USB external hard disk drive:

Target Device: Seagate(TM) Expansion SCSI Disk Device
Port: USB 3.0
Vendor: Seagate
Model: 2321
Description: Seagate Expansion USB Device

Solution: This hot fix updates the Data Loss Prevention Endpoint SDK 6.0 module of the OfficeScan 11.0 agent program to enable it to support the external hard disk drive described above which appears as a SCSI drive.

Enhancement: This hot fix enables the Data Loss Prevention Endpoint SDK 6.0 module in OfficeScan 11.0 agents to support some specific USB external hard disk drives that appear as SCSI drives.

Hot Fix Build 3063

Issue: The "days" setting in the "Privileges and Other Settings > Cache Settings for Scans" page of the OfficeScan web console automatically resets to "0" after the server deploys the other settings to OfficeScan agents.

Solution: This hot fix updates the OfficeScan 11.0 Service Pack 1 server and agent files to resolve this issue.

Hot Fix Build 3064

Issue 1: When upgrade from an older OfficeScan client version installed using an MSI package, to OfficeScan 11(SP1) agent, you cannot uninstall the agent from the Microsoft(TM) Windows(TM) "Control Panel > Programs and Features" page because it will not accept the correct password. This occurs because OfficeScan 11(SP1) stores the uninstallation password in a different location.

Solution 1: This hot fix enables OfficeScan 11(SP1) agents to store the uninstallation password in the correct location. This ensures that users will be able to uninstall OfficeScan 11(SP1) agents using the correct password through the Windows "Control Panel > Programs and Features" page.

Issue 2: On OfficeScan agents, the Ntrtscan.exe process stops unexpectedly when the Real-time Scan service starts.

Solution 2: This hot fix updates the OfficeScan agent program to ensure that the Ntrtscan.exe process runs normally when the Real-time Scan service starts.

Issue 3: When users deploy an OfficeScan policy from a Trend Micro Control Manager(TM) 6.0 server, the "Approved Programs" list under the Behavior Monitoring setting displays truncated path names. The path names may be truncated after the first "P" or "T" character.

Solution 3: This hot fix updates the OfficeScan program to ensure that the complete path names appear in the "Approved Programs" list of the Behavior Monitoring setting.

Hot Fix Build 3065

Issue: An issue with the Trend Micro Data Loss Prevention(TM) (DLP) validator mapping in the "UK: RD&E Hospital Number" may prevent the DLP rule from blocking some restricted information.

Solution: This hot fix ensures that OfficeScan uses the correct DLP validator in the "UK: RD&E Hospital Number" template.

Hot Fix Build 3067

Issue: Sometimes, Trend Micro Control Manager(TM) cannot retrieve information about OfficeScan clients from an OfficeScan server in SQL mode.

Solution: After applying this hot fix, Control Manager bypasses the synchronization when the OfficeScan server cannot connect to the SQL server while in SQL mode.

Hot Fix Build 3068

Issue: When multiple OfficeScan agents register to the OfficeScan server with the agent grouping rule enabled, the GenerateSAF process may prevent new OfficeScan agents from registering to the OfficeScan server.

Solution: This hot fix resolves this issue so that new OfficeScan agents can register to the OfficeScan server successfully.

Hot Fix Build 3069

Issue: A timing issue can cause the AutoPCC process and the OfficeScan agent TmListen or NtrtScan process to start at almost the same time. When this happens, component updates may fail because the TmListen or NtrtScan cannot be stopped.

Solution: This hot fix enables users to set how long the AutoPCC process should wait for the TmListen or NtrtScan to start before attempting to stop these processes which can help resolve the timing issue.

Hot Fix Build 3070

Issue: The OfficeScan Common Client Solution Framework (CCSF) Anti-Malware solution platform module may trigger a handle leak issue.

Solution: This hot fix updates the CCSF Anti-Malware solution platform module in OfficeScan 11.0 Service Pack 1 to solve the handle leak issue.

Hot Fix Build 3071

Enhancement: Trend Micro released this hot fix in response to recent widespread ransomware attacks.

Upon detecting a newly encountered program downloaded through HTTP or email applications, OfficeScan temporarily blocks the program and prompts users to select an action

("Block Once" or "Allow Once"). If users do not select an action within the specified time period, the program is automatically blocked.

In the previous version of OfficeScan, the monitoring of newly encountered programs is disabled by default. This feature is configurable in the Global Agent Settings screen.

For more information about ransomware, visit the following Trend Micro web page: http://www.trendmicro.com/vinfo/us/security/definition/Ransomware.

Hot Fix Build 3072

Issue: The name of and paths to infected files cannot be displayed correctly in outbreak email notifications from OfficeScan.

Solution: This hot fix updates the OfficeScan server files to ensure that outbreak email notifications always contain and display complete and accurate information.

Hot Fix Build 3073

Issue: On the Chinese, Japanese, and Korean (CJK) versions of the Microsoft(TM) Windows(TM) platform, Data Loss Prevention Endpoint may not be able to detect the transfer of sensitive files in Google Chrome.

Solution: This hot fix ensures that Data Loss Prevention Endpoint can successfully detect and block the transfer of sensitive files in Google Chrome.

Hot Fix Build 3074

Issue: OfficeScan agents that have been assigned specific IP addresses using the IP template may not be able to report a valid MAC address to the OfficeScan server.

Solution: This hot fix ensures that these OfficeScan agents can report valid MAC addresses to the OfficeScan server.

Hot Fix Build 3076

Issue: After installing a hot fix or patch, the OfficeScan agent from updating the build number in the corresponding registry key or may trigger it to update the information to the wrong value. As a result, the wrong build number appears in the "Windows Control Panel > Programs > Programs and Features > Version" tab.

Solution: This hot fix resolves the issue to ensure that OfficeScan 11 agents promptly and correctly update the build number information in the corresponding registry key after a successful hot fix or patch installation.

Hot Fix Build 3076.1

Issue: The Trend Micro Control Manager(TM) "Isolate" and "Restore" commands do not work properly on an OfficeScan client that is not protected by a firewall and trigger an error message on the OfficeScan client console.

Solution: This hot fix resolves the error by ensuring that OfficeScan sends the correct status codes for the "Isolate" and "Restore" commands to Control Manager.

Hot Fix Build 3077

Issue: When CGI applications become unresponsive due to multiple agent requests in the queue, the OfficeScan server master service stops accepting new requests from agents.

Solution: This hot fix updates the master service module to resolve this issue.

Hot Fix Build 3078

Enhancement: This hot fix enables the OfficeScan 11.0 server to download the list of approved USB devices of the Device Control Settings from the Trend Micro Control Manager(TM) server and to deploy the list to OfficeScan agents.

The list of approved USB devices supports up to 18,000 devices.

Hot Fix Build 3079

Issue: An issue related to the OfficeScan Browser Exploit Solution feature triggers Microsoft(TM) Internet Explorer(TM) to stop unexpectedly when users open a Microsoft Word document using a web application.

Solution: This hot fix ensures that the OfficeScan Browser Exploit Solution feature works well with Internet Explorer.

Hot Fix Build 3081

Issue: An issue related to the OfficeScan iCRC common module may trigger the computer to slow down and stop responding.

Solution: This hot fix updates the OfficeScan iCRC common module to resolves the performance issue.

Hot Fix Build 3081.1

Issue: When Data Loss Prevention (DLP) is enabled in OfficeScan, the Copy File Path function does not work in Visual Studio.

Solution: This hot fix provides the "clipboard_idle_time" setting that allows users to configure DLP to wait for a specified time (in seconds) to prevent DLP from accessing the clipboard data at the same time as Visual Studio.

Hot Fix Build 3082

Issue: After an OfficeScan 11 agent that was installed using an MSI package is upgraded to OfficeScan 11 Service Pack 1, the agent program cannot be uninstalled from the Microsoft(TM) Windows(TM) "Control Panel > Programs and Features" page because it will not accept the correct password.

Solution: This hot fix updates the OfficeScan program to ensure that users will be able to uninstall OfficeScan 11 Service Pack 1 agents using the correct password through the Windows "Control Panel > Programs and Features" page.

Hot Fix Build 3083

Issue: The OfficeScan server cannot apply the firewall policy to an OfficeScan client if the client's IP address is retrieved using certain VPN client programs.

Solution: This hot fix updates the OfficeScan server and client programs to ensure that the OfficeScan server can successfully apply the firewall policy to clients.

Hot Fix Build 3084

Issue: If the OfficeScan server receives a request from an OfficeScan agent and the MAC address field is empty, the server matches the empty MAC address to all the other existing agent MAC addresses. As a result, the OfficeScan server treats these addresses as duplicates and deletes all the existing agent MAC addresses.

Solution: This hot fix enables the OfficeScan server to skip the check for duplicate MAC addresses when it receives a request with an empty MAC address field.

Hot Fix Build 3085

Issue: After upgrading to OfficeScan 11 Service Pack 1, the OfficeScan Master Service may not be able to start because the Trend Micro Active Update (AU) module cannot start successfully.

Solution: This hot fix allows users to enable the AU module to check certificates to help ensure that the module can start successfully.

Hot Fix Build 3087

Issue: Users may not be able to restore or update the configuration of an OfficeScan client that has been placed on network quarantine. This happens when the OfficeScan client cannot resolve the OfficeScan server's IP address which prevents the firewall rule 10208 from working. When this happens, the client cannot receive configuration updates.

Solution: This hot fix adds a rule that allows DNS traffic to pass through during the firewall initialization process. This ensures that OfficeScan clients that are in network quarantine can still receive configuration updates.

Hot Fix Build 3088

Enhancement: This hot fix enables the OfficeScan 11.0 server to download the list of approved USB devices of the Device Control Settings from the Trend Micro Control Manager(TM) server and to deploy the list to OfficeScan agents.

The list of approved USB devices supports up to 18,000 devices.

Hot Fix Build 3089

Issue: The Trend Micro Behavior Monitoring feature may block OfficeScan agent computers from running files that are saved in a shared network drive.

Solution: This hot fix resolves the issue to ensure that OfficeScan agent computers can successfully run files from shared network drives.

Hot Fix Build 3091

Enhancement 1: This hot fix enables Data Loss Prevention(DLP) Endpoint to monitor inline response events in Microsoft(TM) Outlook(TM) 2013 including "Reply", "Reply all", and "Forward" events.

Enhancement 2: This hot fix enables Data Loss Prevention(DLP) Endpoint support blocking Yahoo Mail using SPDY protocol.

Hot Fix Build 3099

Issue 1: Sometimes, the status of the Trend Micro Data Loss Protection(TM) service appears as "Stopped" in the OfficeScan agent console but appears as "Running" on the "Agent Management" page of the OfficeScan web console.

Solution 1: This hot fix ensures that the Data Loss Prevention status on the OfficeScan web console "Agent Management" page is consistent with the information on the OfficeScan agent console.

Issue 2: The TMEBC driver fails to start during the system boot process because the TMEBC driver file (TMEBC32.SYS on x86 platforms or TMEBC64.SYS on x64 platforms) is not in the C:¥Windows¥system32¥DRIVERS directory while the corresponding registry entry still exists on the Services screen.

Solution 2: This hot fix resolves this issue by installing the TMEBC driver on OfficeScan clients if the TMEBC driver is not installed or if the TMEBC driver file is missing.

Hot Fix Build 3100

Issue: The following error message appears after users isolate an OfficeScan client from the Trend Micro Control Manager(TM) endpoint page even when the client was isolated successfully:

"Unable to isolate the endpoint. Both the OfficeScan server and agent are installed on the endpoint. Isolation the endpoint will cause disruptions to OfficeScan server functions."

This happens when the OfficeScan server does not receive the isolation status from the client which prompts it to send the wrong status to Control Manager.

Solution: This hot fix resolves the issue by ensuring that OfficeScan clients promptly send the correct isolation status to the server.

Hot Fix Build 3101

Issue: The "Scan all files in removable storage devices after plugging in" setting reverts to the default value after the OfficeScan client runs an update now task.

Solution: This hot fix ensures that the "Scan all files in removable storage devices after plugging in" setting does not change unexpectedly after OfficeScan client runs an update now task.

Hot Fix Build 3107

Enhancement 1: This hot fix enables Data Loss Prevention(DLP) Endpoint to avoid start up issues of guest hosts on Oracle(TM) VirtualBox(TM) when the DLP service has been started.

Enhancement 2: This hot fix enables Data Loss Prevention(DLP) Endpoint to not block Dropbox's uploading of application logs to Dropbox backend.

Enhancement 3: This hot fix enables Data Loss Prevention(DLP) Endpoint to detect a specific SD card reader.

Hot Fix Build 3111

Issue 1: The OfficeScan Data Loss Prevention(TM) (DLP) module cannot detect a certain keyword in CSV files.

Solution 1: This hot fix ensures that the OfficeScan DLP module can detect keywords in CSV files.

Issue 2: An issue in the OfficeScan DLP module may trigger some applications to stop unexpectedly while the computer prints documents.

Solution 2: This hot fix resolves the issue to ensure that users can print documents on protected computers without issues.

Hot Fix Build 3113

Issue: An issue related to the "tmeectv.dll" module in OfficeScan 11.0 Service Pack 1 may trigger a handle leak issue.

Solution: This hot fix updates the OfficeScan 11.0 Service Pack 1 agent files to prevent the handle leak issue.

Hot Fix Build 3596

Enhancement: Trend Micro released this hot fix in response to recent widespread ransomware attacks.

Upon detecting a newly encountered program downloaded through HTTP or email applications, OfficeScan temporarily blocks the program and prompts users to select an action ("Block Once" or "Allow Once"). If users do not select an action within the specified time period, the program is automatically blocked.

In the previous version of OfficeScan, the monitoring of newly encountered programs is disabled by default. This feature is configurable in the Global Agent Settings screen.

For more information about ransomware, visit the following Trend Micro web page: http://www.trendmicro.com/vinfo/us/security/definition/Ransomware.

Hot Fix Build 3600

Issue: The OfficeScan 11 Service Pack 1 package contains an older version of "OfcCMAgent.exe".

Solution: This hot fix updates the "OfcCMAgent.exe" file in the OfficeScan 11 Service Pack 1 package to the correct version.

Hot Fix Build 3602

Issue: The OfficeScan server promptly sends out an email notification when it detects a command & control (C&C) callback event. However, the information in the C&C list source column on the email notification may not be accurate.

Solution: This hot fix ensures that the C&C callback event email notifications contain complete and accurate information.

Hot Fix Build 3603

Issue 1: The OfficeScan Data Loss Prevention(TM) (DLP) module cannot detect a certain keyword in CSV files.

Solution 1: This hot fix ensures that the OfficeScan DLP module can detect keywords in CSV files.

Issue 2: An issue in the OfficeScan DLP module may trigger some applications to stop unexpectedly while the computer prints documents.

Solution 2: This hot fix resolves the issue to ensure that users can print documents on protected computers without issues.

Hot Fix Build 3606

Issue: OfcService.exe may stop unexpectedly when a library file is unloaded while other threads are still using it.

Solution: This hot fix helps prevent the issue by allowing users to configure OfficeScan to automatically kill threads that have timed-out.

Hot Fix Build 3607

Issue: Sometimes, the OfficeScan TmListen service triggers a high CPU usage issue.

Solution: This hot fix updates the TMUFE engine to prevent the high CPU usage issue.

Hot Fix Build 3608

Issue: The OfficeScan agent indicates that the iDLP service is running but in reality the service is stopped.

Solution: This hot fix enables the Data Loss Prevention(DLP) Endpoint to send status report to Windows Service Control Manager. The service also sets the timeout when the service starts up.

Hot Fix Build 3611

Issue: OfficeScan clients that are installed on Microsoft(TM) Windows(TM) Server 2012 R2 with Domain Controller are displayed as "WindowsNT Platform Series" on the agent management tree. This happens because the Window API uses a stand-alone type to indicate the domain controller server and some OfficeScan server programs cannot handle this type.

Solution: This hot fix enables OfficeScan to handle domain controller server types so it can display the correct information on the agent management tree.

Enhancement: This hot fix ensures that OfficeScan displays Trend Micro Data Loss Prevention(TM) violation notification pop ups in the correct session by enabling it to check if the user name in the pop up window matches the login name for the current session before displaying the pop up.

Hot Fix Build 3612

Issue: Users may encounter the "Unknown error. Please try again." message when saving changes to the Real-time Scan Settings of a particular domain. This occurs when OfficeScan attempts to convert an empty string.

Solution: This hot fix updates the OfficeScan 11.0 server and agent files so users can successfully edit and save the Real-time Scan Settings for domains.

Hot Fix Build 3612

Issue: The Trend Micro Control Manager(TM) Agent (CMAgent) stops unexpectedly when it encounters a null XML object.

Solution: This hot fix updates the OfficeScan server file to prevent the CMAgent from stopping unexpectedly when it encounters a null XML object.

Hot Fix Build 3613

Issue: The OfficeScan agent's NtrtScan.exe process crashes when it calls Data Loss Prevention's (DLP) TmDlpeGetCurrentDiscVersion function.

Solution: This hot fix updates the DLP module of the OfficeScan agent which validates the pointer before accessing its method.

Hot Fix Build 3615

Issue: Users may not be able to access any web site shortly after enabling the Web Reputation Service (WRS). This occurs because the TMCCSF IPC server stops unexpectedly and prevents TmProxy from sending IPC commands to the TMCCSF service. Users can work around this by disabling WRS or unloading the OfficeScan client.

Solution: This hot fix resolves the issue by enabling the TMCCSF service to start the IPC server if it detects that the server has stopped working.

Hot Fix Build 3618

Issue: Users cannot edit or delete scheduled scan tasks for the Vulnerability Scanner when there are more than 10 scheduled scan tasks.

Solution: This hot fix updates the OfficeScan files to ensure that users can successfully edit and delete Vulnerability Scanner scheduled scan tasks without affecting any of the other related settings.

Hot Fix Build 3621

Enhancement: This hot fix enables users to create a list of approved URLs for the Osprey module and to deploy the list globally.

Hot Fix Build 3624

Issue: The OfficeScan web console does not allow users to save more than 248 exceptions in a firewall policy.

Solution: This hot fix updates the OfficeScan server and agent programs to allow users to successfully save more than 248 exceptions in a firewall policy.

Hot Fix Build 3625

Issue: The AEGIS module included in the OfficeScan agent may cause some processes to become unresponsive when the system resumes operation from sleep mode.

Solution: This hot fix updates the AEGIS module with the AntiHangLoose feature that resolves this issue.

Hot Fix Build 3626

Issue: The AEGIS module included in the OfficeScan agent may cause some processes to become unresponsive when the system resumes operation from sleep mode.

Solution: This hot fix updates the AEGIS module with the AntiHangLoose feature that resolves this issue.

Hot Fix Build 3629

Issue: An incompatibility issue between the OfficeScan Advanced Protection Service and Microsoft(TM) Internet Explorer(TM) can prevent users from downloading and viewing .xdw files in the browser.

Solution: This hot fix ensures that the OfficeScan Advanced Protection Service works well with Internet Explorer.

Hot Fix Build 3634

Issue: When the OfficeScan client detects system events while the "EnableEventLog" option is enabled, the corresponding NT event logs do not appear in the Microsoft(TM) Windows(TM) event log file.

Solution: This hot fix ensures that when OfficeScan clients detect system events while the "EnableEventLog" option is enabled, the OfficeScan client NT event log function adds the corresponding NT event log to the Windows event log file.

Hot Fix Build 3639

Issue: The Spyware/Grayware Approved List on the OfficeScan server web console is case-sensitive which prevents OfficeScan from recognizing and allowing spyware and grayware names that are upper or lowercase variants of the items on the list.

Solution: This hot fix makes the Spyware/Grayware Approved List case-insensitive to allow OfficeScan to recognize and allow upper and lowercase variants of the items on the list.

Hot Fix Build 3640

Issue 1: The OfficeScan server sends out standard and outbreak notifications without any scan type information.

Solution 1: This hot fix adds an option to add scan type information in standard and outbreak notifications from the OfficeScan server.

Issue 2: An issue prevents OfficeScan 11.0 Service Pack 1 from locating and running a manual scan on remote drives by using the command.

Solution 2: This hot fix ensures that OfficeScan 11.0 Service Pack 1 can locate and running manual scans on remote drives.

Hot Fix Build 3641

Issue 1: The OfficeScan Data Loss Prevention(TM) (DLP) module cannot block SD card reader attached on parent device with SCSI¥PCI prefix.

Solution 1: This hot fix provides additional support for specific SD card reader attached on parent device with SCSI¥PCI prefix.

Issue 2: The OfficeScan Data Loss Prevention(TM) (DLP) module cannot block the .prt files.

Solution 2: This hot fix import dtSearch 7.81.8271 to support new format of .prt files.

Hot Fix Build 3642

Issue 1: OfficeScan Data Loss Prevention(TM)(DLP) takes a long time to copy files from Microsoft(TM) Outlook(TM) 2010 to a USB stick.

Solution 1: This hot fix ensures that users can copy files normally from Outlook 2010 to a USB stick.

Issue 2: OfficeScan Data Loss Prevention(TM)(DLP) unable to block sensitive file upload to Dropbox by using Google Chrome.

Solution 2: This hot fix ensures can block sensitive file upload to Dropbox by using Google Chrome.

Hot Fix Build 3645

Issue: Sometimes, the OfficeScan Master Service stops unexpectedly while the OfficeScan server retrieves policies from Trend Micro Control Manager(TM).

Solution: This hot fix ensures that the OfficeScan server can retrieve policies from Control Manager successfully.

Enhancement: This hot fix enables users to configure the OfficeScan server to notify agents to retrieve and apply configuration updates without waiting for a notification from the Update Agent.

Hot Fix Build 3647

Issue: OfficeScan Data Loss Prevention(TM) has compatibility issues with Dragon NaturallySpeaking software.

Solution: This hot fix updates OfficeScan Data Loss Prevention(TM) to resolve this compatibility issue.

Hot Fix Build 3649

v

Issue: OfficeScan Data Loss Prevention(TM) cannot block the sensitive file copied from shared folder.

Solution: This hot fix ensures OfficeScan Data Loss Prevention(TM) can block the sensitive file from SMB server mode.

Hot Fix Build 3650

Issue: The OfficeScan server is unable to perform a Scan Now task with no OfficeScan agents listed in Scan Now console. This situation occurs if the domain name contains a single quote symbol (').

Solution: This hot fix ensures that the OfficeScan Scan Now task can perform successfully even when this situation occurs.

Hot Fix Build 3651

Issue: The result from an unmanaged endpoints query is not correct when using an SQL server as the OfficeScan database and the client numbers are large.

Solution: This hot fix ensures the query result of unmanaged endpoints is correct.

Hot Fix Build 3651.1

Issue: The OfficeScan web console is affected by a cross-site scripting (XSS) vulnerability.

Solution: This hot fix updates the OfficeScan web console program to resolve the vulnerability.

Hot Fix Build 3653

Issue: Sometimes, OfficeScan outbreak notification email messages contain truncated file paths.

Solution: This hot fix resolves the truncation issue in OfficeScan outbreak notification email messages.

Hot Fix Build 3655

Issue: This hot fix allows users to configure OfficeScan to display the release date of the current Virus Pattern or Smart Scan Agent Pattern in the component version page of the OfficeScan agent console based on the scan mode.

Hot Fix Build 3659

Issue: When the OfficeScan Data Loss Prevention (DLP) module is run on Microsoft Windows 7 platforms, a blue screen error may occur.

Solution: This hot fix resolves the issue so that the DLP module in OfficeScan does not cause a blue screen error in Microsoft Windows 7.

Hot Fix Build 3673

Issue: Users cannot add the Pandion instant messaging program to the list of approved programs of the Behavior Monitoring Local Pattern in OfficeScan manually.

Solution: This hotfix updates the OfficeScan Behavior Monitoring Local Pattern to add the Pandion instant messaging program to its approved list.

Hot Fix Build 3674

Issue: Virus/Malware logs that were triggered by infection source events do not contain any information about the infection sources.

Solution: This hotfix ensures that Virus/Malware logs that are triggered by infection source events contain information about the specific infection sources.

Hot Fix Build 3679

Issue 1: Launch application like Internet Explorer will cause OfficeScan Data Loss Prevention(TM)(DLP) Blue Screen of Death(BSoD) when Enhanced Mitigation Experience Toolkit(EMET) 5.5 is enabled.

Solution 1: This hot fix bypass the process injected by EMET to resolves the BSoD issue.

Issue 2: OfficeScan Data Loss Prevention(TM)(DLP) not blocked sensitive file uploading to Dropbox web by using Internet Explorer.

Solution 2: This hot fix provide support for Dropbox web upload based on new Dropbox version.

Hot Fix Build 3679.1

Issue: On Microsoft(TM) Windows(TM) 64-bit operating systems, the OfficeScan agent cannot be installed using an MSI package created by the ClientPackager tool if the cabinet file is larger than 300MB.

Solution: This hotfix allows users to adjust the threshold size of cabinet files that the ClientPackager tool generates to help ensure that the OfficeScan agent can be installed properly.

Hot Fix Build 3681

Issue: Domain names that contain garbled characters cannot be displayed correctly in the client tree on the OfficeScan web console.

Solution: This hot fix provides an option to allow users to filter a predefined special keyword such as a special character for the sorting rule. This helps ensure that the OfficeScan server can successfully display domain names in the client tree using Automatic Agent Grouping.

Hot Fix Build 3681

Issue: The OfficeScan "cgiShowClientAdm.exe" and "cgiShowServerAdm.exe" processes are vulnerable to XSS.

Solution: This hotfix updates the OfficeScan 11.0 Service Pack 1 program to enable it to filter out special characters in process parameters to prevent XSS.

Hot Fix Build 3682

Issue: It may take a long time for users to log on to computers running on the Windows platform when the "Delay the RealTime Scan service from starting at startup" feature of the OfficeScan 11.0 Service Pack 1 agent program is enabled.

Solution: This hotfix updates the OfficeScan agent program to prevent the performance issue and ensure that users can log on to protected computers normally.

Hot Fix Build 3683

Issue: If for some reason an OfficeScan client fails to send virus logs to the server, the client will keep trying to send the logs until it succeeds or it has reached a hard-coded number of times. A user requests for a way to configure this value manually.

Solution: This hotfix allows users to manually configure the maximum number of times an OfficeScan client should attempt to send virus logs to the OfficeScan server if it encounters issues sending the logs.

Enhancement: This hotfix contains new versions of the "Trend Micro NSC Firefox Extension" and "Trend Micro Osprey Firefox Extension". These versions comply with the new security guidelines.

Hot Fix Build 3689

Issue: When an OfficeScan server receives a policy from Control Manager(TM) it notifies all clients within the policy's scope instead of sending the notification only to specific clients.

Solution: This hotfix enables the OfficeScan server to deploy the policy settings to specific clients.

Hot Fix Build 3690

Enhancement: This hotfix enables the OfficeScan DLP module to show the file size information in violation logs.

Hot Fix Build 3692

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 3697

Enhancement: This hotfix enables OfficeScan to send the login password to connect to the Control Manager server by "POST" method.

Hot Fix Build 4151

Issue: After users install the OfficeScan 11 Service Pack 1 with Critical Patch 4150 (with Microsoft(TM) Windows(TM) 10 support) agent on a computer running Windows 10, the computer restarts when users attempt to shut it down.

Solution: This hot fix resolves the issue by deploying an updated Trend Micro Eagle Eye file to all OfficeScan agents that are managed by the OfficeScan server.

Hot Fix Build 4164

Issue: The "days" setting in the "Privileges and Other Settings > Cache Settings for Scans" page of the OfficeScan web console automatically resets to "0" after the server deploys the other settings to OfficeScan agents.

Solution: This hot fix updates the OfficeScan 11.0 Service Pack 1 server file to resolve this issue.

Hot Fix Build 4165

Issue: When upgrade from an older OfficeScan client version installed using an MSI package, to OfficeScan 11(SP1) agent, you cannot uninstall the agent from the Microsoft(TM) Windows(TM) "Control Panel > Programs and Features" page because it will not accept the correct password. This occurs because OfficeScan 11(SP1) stores the uninstallation password in a different location.

Solution: This hot fix enables OfficeScan 11(SP1) agents to store the uninstallation password in the correct location. This ensures that users will be able to uninstall OfficeScan 11(SP1) agents using the correct password through the Windows "Control Panel > Programs and Features" page.

Hot Fix Build 4165.1

Issue: If the OfficeScan server uses an SQL database, the contents of Scan Exclusion List (Directories) and Scan Exclusion List (Files) are removed when administrators select a domain and save the Scan Exclusion settings.

Solution: This hot fix resolves this issue so that the contents of Scan Exclusion List (Directories) and Scan Exclusion List (Files) are retained after performing the save operation.

Hot Fix Build 4168

Enhancement: This hot fix enables users to configure a Web Reputation policy for agents running Microsoft(TM) Windows(TM) Server 2003, Windows Server 2008, or Windows Server 2012 by selecting the root domain icon, specific domains, or specific agents in the "Agent Management" page of the OfficeScan web console.

Hot Fix Build 4170

Issue: When the OfficeScan server updates OfficeScan agent settings to the database, the server purges old information without verifying the GUIDs for agents. As a result, OfficeScan agents that do not have a previous GUID entry in the database revert to default settings.

Solution: This hot fix adds a GUID checking mechanism that enables the OfficeScan server to verify if a particular agent GUID exists in the agent table of the database before updating the agent information. If a GUID does not exist in the agent table, the OfficeScan server returns an error message and does not overwrite the agent settings.

Hot Fix Build 4171

Issue 1: When users deploy an OfficeScan policy from a Trend Micro Control Manager(TM) 6.0 server, the "Approved Programs" list under the Behavior Monitoring setting displays truncated path names. The path names may be truncated after the first "P" or "T" character.

Solution 1: This hot fix updates the OfficeScan program to ensure that the complete path names appear in the "Approved Programs" list of the Behavior Monitoring setting.

Issue 2: The name of and paths to infected files cannot be displayed correctly in outbreak email notifications from OfficeScan.

Solution 2: This hot fix updates the OfficeScan server files to ensure that outbreak email notifications always contain and display complete and accurate information.

Issue 3: The Trend Micro Data Loss Prevention(TM) (DLP) module of the OfficeScan agent program cannot detect the transfer of sensitive information when the OfficeScan agent self-protection function is enabled.

Solution 3: This hot fix updates the OfficeScan agent program to ensure that the DLP module can successfully detect the transfer of sensitive information.

Issue 4: Sometimes, an OfficeScan agent encounters performance issues when its Damage Cleanup Services (DCS)(TSC.exe) checks the digital signature of files and the Microsoft(TM) Windows(TM) certificate on the agent computer is outdated.

Solution 4: This hot fix allows users to prevent DCS from checking digital signatures.

Hot Fix Build 4172 and Hot Fix Build 4779

Enhancement: Trend Micro released this hot fix in response to recent widespread ransomware attacks.

Upon detecting a newly encountered program downloaded through HTTP or email applications, OfficeScan temporarily blocks the program and prompts users to select an action

("Block Once" or "Allow Once"). If users do not select an action within the specified time period, the program is automatically blocked.

In the previous version of OfficeScan, the monitoring of newly encountered programs is disabled by default. This feature is configurable in the Global Agent Settings screen.

For more information about ransomware, visit the following Trend Micro web page: http://www.trendmicro.com/vinfo/us/security/definition/Ransomware.

Hot Fix Build 4175

Issue: When users trigger the "Scan Now" feature of an OfficeScan agent to run a manual scan, some drives do not appear in the scan folder selection box.

Solution: This hot fix updates some OfficeScan files to ensure that the scan folder selection box displays all drives under the scenario described above.

Hot Fix Build 4176

Issue: A timing issue can cause the AutoPCC process and the OfficeScan agent TmListen or NtrtScan process to start at almost the same time. When this happens, component updates may fail because the TmListen or NtrtScan cannot be stopped.

Solution: This hot fix enables users to set how long the AutoPCC process should wait for the TmListen or NtrtScan to start before attempting to stop these processes which can help resolve the timing issue.

Hot Fix Build 4176.1

Issue: OfficeScan 11.0 service pack 1 with Critical Patch 4150 may not be able to recognize token variables in the "Subject" field of C&C callback notification email messages. As a result, the token names appear instead of the corresponding information.

Solution: This hot fix ensures that OfficeScan 11.0 service pack 1 with Critical Patch 4150 recognizes token variables in the "Subject" field of C&C callback notification email messages and replaces these variables with the correct information.

Hot Fix Build 4177 merfed from Hot Fix Build 1799

Issue 1: The OfficeScan NT RealTime Scan service may cause the system to become unresponsive when running in conjunction with the Behavior Monitoring feature.

Solution 1: This hot fix updates the OfficeScan agent files which ensures that the Realtime Scan service does not cause the system to become unresponsive.

Issue 2: Some OfficeScan agents keep launching "upgrade.exe" because the OfficeScan server repeatedly sends several notifications for changes in the Scan Methods settings even when there are no changes.

Solution 2: This hot fix updates the OfficeScan server program to ensure that it sends the correct notifications to OfficeScan agents.

Hot Fix Build 4178

Issue: On OfficeScan agents, the Ntrtscan.exe process stops unexpectedly when the Real-time Scan service starts.

Solution: This hot fix updates the OfficeScan agent program to ensure that the Ntrtscan.exe process runs normally when the Real-time Scan service starts.

Hot Fix Build 4179

Issue: The Trend Micro Control Manager(TM) "Isolate" and "Restore" commands do not work properly on an OfficeScan client that is not protected by a firewall and trigger an error message on the OfficeScan client console.

Solution: This hot fix resolves the error by ensuring that OfficeScan sends the correct status codes for the "Isolate" and "Restore" commands to Control Manager.

Hot Fix Build 4180

Issue: On OfficeScan agents, the Ntrtscan.exe process stops unexpectedly when the Real-time Scan service starts.

Solution: This hot fix updates the OfficeScan agent program to ensure that the Ntrtscan.exe process runs normally when the Real-time Scan service starts.

Hot Fix Build 4182

Enhancement: This hot fix enables the OfficeScan 11.0 server to download the list of approved USB devices of the Device Control Settings from the Trend Micro Control Manager(TM) server and to deploy the list to OfficeScan agents.

The list of approved USB devices supports up to 18,000 devices.

Hot Fix Build 4186

Issue: The TCacheGenCli tool does not respond to the "REMOVE_GUID" command.

Solution: This hot fix ensures that the TCacheGenCli tool responds normally to the "REMOVE_GUID" command.

Hot Fix Build 4187 and Hot Fix Build 4792.1

Issue: If the OfficeScan server receives a request from an OfficeScan agent and the MAC address field is empty, the server matches the empty MAC address to all the other existing agent MAC addresses. As a result, the OfficeScan server treats these addresses as duplicates and deletes all the existing agent MAC addresses.

Solution: This hot fix enables the OfficeScan server to skip the check for duplicate MAC addresses when it receives a request with an empty MAC address field.

Hot Fix Build 4188

Issue: If the OfficeScan server uses an SQL database, policy settings that were deployed from the Trend Micro Control Manager(TM) server to multiple OfficeScan agents are applied to only one of the target agents.

Solution: This hot fix ensures that policy settings that are deployed from the Control Manager server are successfully applied to all target OfficeScan agents.

Hot Fix Build 4190

Issue: After upgrading to OfficeScan 11 Service Pack 1 with Critical Patch 4150, the OfficeScan Master Service may not be able to start because the Trend Micro Active Update (AU) module cannot start successfully.

Solution: This hot fix allows users to enable the AU module to check certificates to help ensure that the module can start successfully.

Hot Fix Build 4190

Enhancement:

This hot fix enables the AU module to check certificates.

Hot Fix Build 4191 and Hot Fix Build 4797

Issue 1: After installing a hot fix or patch, the OfficeScan agent from updating the build number in the corresponding registry key or may trigger it to update the information to the wrong value. As a result, the wrong build number appears in the "Windows Control Panel > Programs > Programs and Features > Version" tab.

Solution 1: This hot fix resolves the issue to ensure that OfficeScan 11 agents promptly and correctly update the build number information in the corresponding registry key after a successful hot fix or patch installation.

Issue 2: Sometimes, an OfficeScan agent encounters performance issues when its Damage Cleanup Services (DCS) (TSC.exe) checks the digital signature of files and the Microsoft(TM) Windows(TM) certificate on the agent computer is outdated.

Solution 2: This hot fix allows users to prevent DCS from checking digital signatures.

Hot Fix Build 4192

Enhancement: This hot fix allows users to hide the "Unlock" button on the OfficeScan client console.

Hot Fix Build 4200

Issue: When the scan operation file becomes corrupted for an unknown reason, it may cause the OfficeScan NT Listener service to crash during the OfficeScan agents upgrade.

Solution: This hot fix enables OfficeScan agents to check for invalid records in the scan operation log. If an invalid record is found, the OfficeScan agents will skip the invalid record and migrate to the next record.

Hot Fix Build 4201

Issue: The Data Loss Prevention rule "UK: RD&E Hospi

tal Number" can't detect the number with lower case.

Solution: This hot fix the validator in "UK: RD&E Hospital Number". Let the DLP Agent can detect the number without issues.

Enhancement: This hot fix enables Data Loss Prevention Endpoint support generic url-encoded form post.

Hot Fix Build 4202

Issue: When an OfficeScan 11 Service Pack 1 agent is configured not to upload firewall logs, it may automatically start uploading these logs after restarting.

Solution: This hot fix ensures that OfficeScan agents upload firewall logs only when enabled to do so.

Hot Fix Build 4203

Issue 1: Oracle(TM) VirtualBox(TM) cannot start up guest hosts if DLP service has been started.

Solution 1: This hot fix enables Data Loss Prevention(DLP) Endpoint to avoid start up issues of guest hosts on Oracle(TM) VirtualBox(TM) when the DLP service has been started.

Issue 2:DLP cannot detect a specific SD card reader.

Solution 2: This hot fix enables Data Loss Prevention(DLP) Endpoint to detect a specific SD card reader.

Hot Fix Build 4205

Issue 1: An issue in the "tmeectv.dll" module in OfficeScan may cause a handle leak.

Solution 1: This hot fix updates the OfficeScan agent files to resolve this issue.

Issue 2: OfficeScan agents installed on Windows 7 platforms and later versions may cause a file server to become unresponsive.

Solution 2: This hot fix updates the OfficeScan agent files to resolve this issue.

Hot Fix Build 4206

Issue: When enable OfficeScan SP1 malware Behavior Blocking for both known and potential threats, it is preventing the Microsoft Onedrive application from updating in Windows 10.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4207

Issue 1: When the file input/output (I/O) task is intercepted by other applications, the OfficeScan agent real-time scanning will not be able to perform the scan task and no error message is triggered.

Solution 1: This hotfix enables OfficeScan agents to check and display the health of real-time scanning on both the agent and server sides.

Issue 2: The following error message appears when users click on the agent count link on the dashboard search page of the OfficeScan web console.

"An error occurred. Make sure your network connection is active and that the OfficeScan service is running. If you encounter this error again, contact your support provider for troubleshooting assistance."

Solution 2: This hot fix extends the cache size for the OfficeScan web console so users can successfully view the agent count information after clicking on the link on the dashboard search page without triggering the error message.

Hot Fix Build 4208

Issue: The OfficeScan server cannot apply the firewall policy to an OfficeScan client if the client's IP address is retrieved using certain VPN client programs.

Solution: This hot fix updates the OfficeScan server and client programs to ensure that the OfficeScan server can successfully apply the firewall policy to clients.

Hot Fix Build 4210 and Hot Fix Build 4693

Issue: An issue with the way OfficeScan handles scan threads may prevent users from transferring OfficeScan agents between OfficeScan servers, trigger an OfficeScan server to stop responding, or cause the NT RealTime Scan service to stop unexpectedly.

Solution: This hot fix updates the OfficeScan server and client files to resolve the scan thread handling issue.

Hot Fix Build 4210.1

Issue: The OfficeScan client cannot successful perform a manual scan on a remote drive that runs on a Microsoft(TM) Windows(TM) XP platform.

Solution: This hot fix ensures that the OfficeScan client successful performs a manual scan on a Microsoft Windows XP remote drive.

Hot Fix Build 4211

Issue: An issue related to the OfficeScan Browser Exploit Solution feature triggers Microsoft(TM) Internet Explorer(TM) 8 to stop unexpectedly when users open a Microsoft Word document using a web application.

Solution: This hot fix ensures that the OfficeScan Browser Exploit Solution feature works well with Internet Explorer 8.

Hot Fix Build 4211.1

Issue 1: In environments where Remote Desktop Protocol (RDP) or Independent Computing Architecture (ICA) is used to connect to a Citrix(TM) terminal server, users may encounter an issue with the OfficeScan agent's Trend Micro Data Loss Prevention(TM) (DLP) add-in that may cause Microsoft(TM) Outlook(TM) to stop responding.

Solution 1: This hot fix updates OfficeScan agent programs which resolve this issue on RDP or ICA connections on the Citrix terminal server environment.

Issue 2: Sometimes, Trend Micro Control Manager(TM) cannot retrieve information about OfficeScan clients from an OfficeScan server in SQL mode.

Solution 2: This hot fix enables the OfficeScan server to allow Control Manager to bypass the synchronization when the OfficeScan server cannot connect to the SQL server in SQL mode.

Hot Fix Build 4213

Issue: After an OfficeScan 11 agent that was installed using an MSI package is upgraded to OfficeScan 11 Service Pack 1 Critical Patch 4150, the agent program cannot be uninstalled from the Microsoft(TM) Windows(TM) "Control Panel > Programs and Features" page because it will not accept the correct password.

Solution: This hot fix updates the OfficeScan program to ensure that users will be able to uninstall OfficeScan 11 Service Pack 1 Critical Patch 4150 agents using the correct password through the Windows "Control Panel > Programs and Features" page.

Hot Fix Build 4215 and Hot Fix Build 4709

Issue: While editing the settings in the "Scan settings" page, users cannot scroll down to select items from the scan exclusion list after selecting the "retain current setting" option.

Solution: This hot fix unlocks the scan exclusion list to allow users to scroll down the list after selecting the "retain current setting" option.

Hot Fix Build 4216, Hot Fix Build 4703, and Hot Fix Build 4719

Issue: The OfficeScan server promptly sends out an email notification when it detects a command & control (C&C) callback event. However, the information in the C&C list source column on the email notification may not be accurate.

Solution: This hot fix ensures that the C&C callback event email notifications contain complete and accurate information.

Hot Fix Build 4217

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4217.1

Issue: Users may not be able to restore or update the configuration of an OfficeScan client that has been placed on network quarantine. This happens when the OfficeScan client cannot resolve the OfficeScan server's IP address which prevents the firewall rule 10208 from working. When this happens, the client cannot receive configuration updates.

Solution: This hot fix adds a rule that allows DNS traffic to pass through during the firewall initialization process. This ensures that OfficeScan clients that are in network quarantine can still receive configuration updates.

Hot Fix Build 4218/4698/4709.1

Issue 1: OfficeScan servers do not send out an SQL Database Unavailable Alert when the SQL connection fails.

Solution 1: This hot fix ensures that the OfficeScan server sends an SQL Database Unavailable Alert when the SQL connection fails.

Issue 2: When the OfficeScan client detects system events while the "EnableEventLog" option is enabled, the corresponding NT event logs do not appear in the Microsoft(TM) Windows(TM) event log file.

Solution 2: This hot fix ensures that when OfficeScan clients detect system events while the "EnableEventLog" option is enabled, the OfficeScan client NT event log function adds the corresponding NT event log to the Windows event log file.

Hot Fix Build 4219

Enhancement: This hot fix ensures that OfficeScan displays Trend Micro Data Loss Prevention(TM) violation notification pop ups in the correct session by enabling it to check if the user name in the pop up window matches the login name for the current session before displaying the pop up.

Hot Fix Build 4220

Issue: The following error message appears after users isolate an OfficeScan client from the Trend Micro Control Manager(TM) endpoint page even when the client was isolated successfully:

"Unable to isolate the endpoint. Both the OfficeScan server and agent are installed on the endpoint. Isolation the endpoint will cause disruptions to OfficeScan server functions."

This happens when the OfficeScan server does not receive the isolation status from the client which prompts it to send the wrong status to Control Manager.

Solution: This hot fix resolves the issue by ensuring that OfficeScan clients promptly send the correct isolation status to the server.

Hot Fix Build 4222

Enhancement: This hot fix enables Data Loss Prevention Endpoint SDK 6.0 to support up to version 46.0.2490.22 of the 32 and 64-bit Google Chrome(TM) web browser.

Hot Fix Build 4224

Issue: The OfficeScan agent Device Control settings is set as "Read" for USB and CD/DVD devices but processes such as dllhost.exe action of modifying the DesiredAccess flag of specific files in the devices is blocked.

Solution: This hot fix updates the Data Protection module to ignore the system action of dllhost.exe modifying the DesiredAccess flag of specific files inside a USB or a CD/DVD.

Hot Fix Build 4225

Issue: The version information for the Web Reputation Patch Pattern is not correctly saved on OfficeScan agents endpoints, resulting in repetitive pattern file downloads and excessive network traffic to the OfficeScan server.

Solution: This hot fix updates the OfficeScan agent to resolve this issue.

Hot Fix Build 4227/4726

Issue: A note that appears in the "Global Agent Settings" page of the Japanese version of the OfficeScan web console translates to the following note in English:

"Does not scan the Compressed file if the size exceeds"

Solution: This hot fix changes the note to translate to "Do not scan files if the decompressed file size exceed X MB".

Hot Fix Build 4227.1

Issue: The OfficeScan server console data protection page does not accept upper case letters as one of the entries in the Non-monitored Targets Exceptions.

Solution: This hot fix enables the OfficeScan server console data protection page to accept upper case letters as one of the entries in the Non-monitored Targets Exceptions.

Hot Fix Build 4228

Enhancement: This hot fix enables Data Loss Prevention Endpoint SDK 6.0 to support up to version 46.0.2490.80 of the 32 and 64-bit Google Chrome(TM) web browser.

Hot Fix Build 4229/4725

Issue: An issue related to the Behavior Monitoring Service module of OfficeScan 11.0 may cause blue screen of death (BSOD).

Solution: This hot fix updates the Behavior Monitoring Service module in OfficeScan 11.0 to prevent the BSOD issue.

Hot Fix Build 4230/4915

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4231/4733.1

Issue 1: The information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan (Scan Now)" fields on the "Agent Management" page of the OfficeScan web console are not updated after a Manual Scan or a Scan Now task completes.

Solution 1: This hot fix updates some OfficeScan files to ensure that the information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan (Scan Now)" fields on the "Agent Management" page of the OfficeScan web console are updated promptly after each virus scan task.

Issue 2: When users upgrade an OfficeScan 10.6 client installed by MSI package to OfficeScan 11 through the "Update Now" function, the value in the "DisplayVersion" registry key is not updated promptly. When this happens, users will not be able to establish a VPN connection trough the Juniper network from the OfficeScan client computer.

Solution 2: This hot fix updates the value of the "DisplayVersion" registry key to ensure that users can successfully establish VPN connections through the Juniper network on affected computers.

Hot Fix Build 4232

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4235

Issue 1: The OfficeScan Data Loss Prevention(TM) (DLP) module cannot block SD card reader attached on parent device with SCSI¥PCI prefix.

Solution 1: This hot fix provides additional support for specific SD card reader attached on parent device with SCSI¥PCI prefix.

Issue 2: The OfficeScan Data Loss Prevention(TM) (DLP) module cannot block the .prt files.

Solution 2: This hot fix import dtSearch 7.81.8271 to support new format of .prt files.

Hot Fix Build 4237

Issue: Logon user names that contain Japanese characters cannot be displayed correctly in the client tree on the OfficeScan web console.

Solution: This hot fix ensures that logon user names that contain Japanese characters are displayed correctly in the client tree on the OfficeScan web console.

Hot Fix Build 4237.1/4753.1

Issue: In the "Agent Management" page of the OfficeScan web console, users cannot create a user account using a user name that contains a period ".".

Solution: This hot fix ensures that users can create user accounts using user names that contain a period "." in the "Agent Management" page of the OfficeScan web console.

Hot Fix Build 4238

Issue: Unexpected matching items were showed in the OfficeScan Data Loss Prevention(TM)(DLP) violation logs.

Solution: This hot fix resolves the unexpected items issue.

Hot Fix Build 4239/4755

Issue: Sometimes, the real-time scan service stops unexpectedly when the OfficeScan agent blocks a newly-inserted USB device.

Solution: This hot fix ensures that the real-time scan service works normally under the scenario described above.

Hot Fix Build 4240

Issue: Sometimes, the "TmListen.exe" service triggers a high CPU usage issue.

Solution: This hot fix updates the OfficeScan agent program to resolve the high CPU usage issue.

Hot Fix Build 4241/4752

Issue: An issue prevents the OfficeScan 11 Update Agent from upgrading an OfficeScan agent from any lower version to version 11.

Solution: This hot fix ensures that the OfficeScan Update Agent can successfully upgrade OfficeScan agents from any lower version to version 11.

Hot Fix Build 4242/4749

Issue: The AEGIS module of the OfficeScan 11.0 agent program may trigger some processes to close unexpectedly.

Solution: This hot fix updates the Behavior Monitoring Service module in OfficeScan 11.0 to ensure that the AEGIS module no longer triggers processes to close unexpectedly.

Hot Fix Build 4243

Issue: When users delete organizational units (OU) from the Active Directory (AD), the OUs remain in the "Custom agent groups" list of OfficeScan domains even when the OUs do not contain any OfficeScan agent.

Solution: This hot fix enables OfficeScan to determine if a deleted AD OU contains any OfficeScan agent, and to delete these from the "Custom agent groups" list if these do not contain any Officescan agent.

Hot Fix Build 4244

Issue: When users make changes through the console of an OfficeScan agent that has the privilege to modify certain OfficeScan server settings, the changes are not applied to the server because the agent provides an incomplete GUID to the server.

Solution: This hot fix updates the OfficeScan agent program to ensure that it provides the complete GUID under the scenario described above.

Hot Fix Build 4245/4756

Issue: OfficeScan clients cannot upload quarantined files to the OfficeScan server because there is a large number of temporary files in the server's temp folder.

Solution: This hot fix cleans the temp folder so that OfficeScan clients can send quarantined files to the OfficeScan server without issues.

Hot Fix Build 4246/4758

Issue: A timing issue can cause the AutoPCC process and the OfficeScan agent TmListen or NtrtScan process to start at almost the same time. When this happens, component updates may fail because the TmListen or NtrtScan cannot be stopped.

Solution: This hot fix enables users to set how long the AutoPCC process should wait for the TmListen or NtrtScan to start before attempting to stop these processes which can help resolve the timing issue.

Hot Fix Build 4247/4759

Issue: An issue prevents OfficeScan 11.0 Service Pack 1 from locating and running a manual scan on remote drives by using the command.

Solution: This hot fix ensures that OfficeScan 11.0 Service Pack 1 can locate and running manual scans on remote drives.

Hot Fix Build 4249/4761

Enhancement: OfficeScan servers deploy Common Firewall Pattern exception rules to all OfficeScan agents. By default, there are up to 5 server IP addresses allowed in GssTrustServer. This hotfix enables users to specify up to 40 server IP addresses for GssTrustServer.

Hot Fix Build 4252/4764

Issue 1: OfficeScan Data Loss Prevention(TM)(DLP) takes a long time to copy files from Microsoft(TM) Outlook(TM) 2010 to a USB stick.

Solution 1: This hot fix ensures that users can copy files normally from Outlook 2010 to a USB stick.

Issue 2: OfficeScan Data Loss Prevention(TM)(DLP) unable to block sensitive file upload to Dropbox by using Google Chrome.

Solution 2: This hot fix ensures can block sensitive file upload to Dropbox by using Google Chrome.

Issue 3: OfficeScan Data Loss Prevention (DLP) is unable to block sensitive file types such as Microsoft(TM) Excel workbooks (*.xlxs) because the DLP function does not extract the contents of the files correctly.

Solution 3: This hot fix ensures that DLP can extract the files correctly and block sensitive content such as Microsoft Excel workbooks.

Hot Fix Build 4253

Issue: OfficeScan may not be able to scan a POP3 email message if the header exceeds a hard-coded length limit.

Solution: This hot fix enables users to set the header length limit for POP3 email messages.

Hot Fix Build 4255

Issue: When the length of a Trend Micro Data Loss Prevention(TM) (DLP) log string exceeds the limit, the OfficeScan master service stops unexpectedly and will not be able to display DLP logs.

Solution: This hot fix updates the OfficeScan file to prevent the OfficeScan master service from stopping unexpectedly and ensure that OfficeScan can display DLP logs properly.

Hot Fix Build 4256/4768

Issue 1: The OfficeScan server sends out standard and outbreak notifications without any scan type information.

Solution 1: This hot fix adds an option to add scan type information in standard and outbreak notifications from the OfficeScan server.

Issue 2: An issue prevents OfficeScan 11.0 Service Pack 1 from locating and running a manual scan on remote drives by using the command.

Solution 2: This hot fix ensures that OfficeScan 11.0 Service Pack 1 can locate and running manual scans on remote drives.

Issue 3: Users can configure the OfficeScan agent Web Reputation Service (WRS) query timeout setting through the OfficeScan server's "ofcscan.ini" file and deploy the setting to agents.

[Global Setting]
RegCount=1
Reg1.Description=WRS Query Timeout: REG_DWORD,HKLM,
SOFTWARE¥TrendMicro¥Osprey¥Scan¥Common

Reg1.Key=!CRYPT!84030FB2DF67D2AF6E912DF0527D84E8D566D98
2932C6EC427ABDFE01658FF2AE03AA3998045B305170E5
C39D028C04437DD883A1485D279549B53AD300797E5415
4F1B480A!41BD912ABF49BD26323972B1B9E545027D0C9
DD5C9AC6E8806ED52E38A6801782C513783D02
Reg1.Value=

OfficeScan agents will sync up the setting to the following registry key:

Path: HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥Osprey
¥Scan¥Common¥URLFilter¥config¥LookupTimeout
Key: flag
Type: DWORD
Value: WRS query timeout value in seconds

However, this key does not deploy correctly to OfficeScan agents which are installed on Microsoft(TM) Windows(TM) x64 platforms.

Solution 3: This hot fix resolves the issue so that users can configure the WRS query timeout setting through the OfficeScan server's "ofcscan.ini" file and deploy the setting to agents properly.

Hot Fix Build 4257

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4258

Issue: OfficeScan's list of approved spyware and grayware contains the names of files and applications that users do not want OfficeScan to treat as spyware or grayware, however, OfficeScan may keep treating a particular file or application on the list as spyware or grayware.

Solution: This hot fix updates the OfficeScan server and agent programs to ensure that OfficeScan does not treat any file or application on the approved list as spyware or grayware.

Hot Fix Build 4259

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4260

Issue: OfficeScan agents add a large number of logs to the "Tminstall.log" file each time the agents update the web reputation settings from the OfficeScan server.

Solution: This hot fix enables users to configure OfficeScan agents to add only the logs for the following two events to the "Tminstall.log" file:

- the TmIEPlugInBHO plug-in is installed for the first time
- the OfficeScan agent is uninstalled

When enabled, this feature can help limit the size of the "Tminstall.log" file.

Hot Fix Build 4262

Issue 1: The OfficeScan Data Loss Prevention(TM)(DLP) module generates a large number of logs when it detects a large illegal file that is attached to a webmail.

Solution 1: This hot fix enables users to set a time interval within which the OfficeScan DLP module will skip events triggered by the same file and will not generate logs for these events.

Issue: The OfficeScan DLP module may not be able to block sensitive files sent through Yahoo(TM) Mail.

Solution 2: This hot fix ensures that the OfficeScan DLP module to block sensitive files sent through Yahoo Mail.

Hot Fix Build 4269/4785.1/4789

Issue: A large number of old files accumulate in the "OfficeScan installation path¥Web¥Service¥AU_Data¥ AU_Storage" folder when the ActiveUpdate module encounters a merge error.

Solution: This hot fix updates the ActiveUpdate module to ensure that it deletes unnecessary update folders from the "OfficeScan installation path¥Web¥Service¥AU_Data¥ AU_Storage" folder.

Hot Fix Build 4270/4782

Issue: A large number of old files accumulate in the "OfficeScan installation path¥Web¥Service¥AU_Data¥ AU_Storage" folder when the ActiveUpdate module encounters a merge error.

Solution: This hot fix updates the ActiveUpdate module to ensure that it deletes unnecessary update folders from the "OfficeScan installation path¥Web¥Service¥AU_Data¥ AU_Storage" folder.

Hot Fix Build 4272

Enhancement: This hot fix adds an option to enable OfficeScan to support Microsoft(TM) Network Access Protection.

After applying this hot fix,users can configure the Trend Micro OfficeScan Security Validator to restrict network access of OfficeScan clients that do not comply with the following settings: Virus pattern is up-to-date (Smart Agent pattern is included).

Hot Fix Build 4273/4781

Enhancement: This hot fix adds Trend Micro Behavior Monitor, hooking Microsoft Windows X86 ZwMapViewOfSection for ransomware detection.

Hot Fix Build 4274

Issue 1: When an IP address is moved to scan exceptions from the Suspicious Object list on Control Manager, Suspicious Object lists on OfficeScan agents are not updated after deployment. This results in false C&C detections on OfficeScan agent endpoints.

Solution 1: This hot fix resolves this issue so that Suspicious Object lists are updated on OfficeScan agents from Control Manager.

Issue 2: The scheduled scanning of OfficeScan agent stops unexpectedly.

Solution 2: This hot fix updates OfficeScan agent's programs and resolves this issue.

Issue 3: When the OfficeScan client POP3 email scan is enabled, users sometimes receive an email with a blank subject, message and sender.

Solution 3: This hot fix resolves this issue.

Issue 4: The result from an unmanaged endpoints query is not correct when using an SQL server as the OfficeScan database and the client numbers are large.

Solution 4: This hot fix ensures the query result of unmanaged endpoints is correct.

Hot Fix Build 4274.1

Issue: The OfficeScan web console is affected by a cross-site scripting (XSS) vulnerability.

Solution: This hot fix updates the OfficeScan web console program to resolve the vulnerability.

Hot Fix Build 4275

Issue: OfficeScan Data Loss Prevention(TM) cannot block the sensitive file copied from shared folder.

Solution: This hot fix ensures OfficeScan Data Loss Prevention(TM) can block the sensitive file from SMB server mode.

Hot Fix Build 4276

Issue: An issue with the Trend Micro Data Loss Prevention(TM) (DLP) validator mapping in the "UK: RD&E Hospital Number" may prevent the DLP rule from blocking some restricted information.

Solution: This hot fix ensures that OfficeScan uses the correct DLP validator in the "UK: RD&E Hospital Number" template.

Hot Fix Build 4277

Issue 1: The Trend Micro Common Client Solution Framework Service may stop responding because of an interoperability issue between SHA256 certificates and a third-party SSL library.

Solution 1: This hot fix updates the related modules to resolve this issue.

Issue 2: Sometimes, the status of the Trend Micro Data Loss Protection(TM) service appears as "Stopped" in the OfficeScan agent console but appears as "Running" on the "Agent Management" page of the OfficeScan web console.

Solution 2: This hot fix ensures that the Data Loss Prevention status on the OfficeScan web console "Agent Management" page is consistent with the information on the OfficeScan agent console.

Issue 3: The TMEBC driver cannot start when the computer starts when the TMEBC driver file ("TMEBC32.SYS" on x86 platforms or "TMEBC64.SYS" on x64 platforms) is missing from the "C:¥Windows¥system32¥DRIVERS" folder and the corresponding registry entry still exists on the "Services" screen.

Solution 3: This hot fix automatically installs the TMEBC driver on OfficeScan clients if the TMEBC driver is not installed or if the TMEBC driver file is missing.

Hot Fix Build 4278/4788

Issue 1: The OfficeScan NT Listener service accesses the "¥Temp¥LogServer" folder frequently which triggers a large number of write operations on the local disk.

Solution 1: This hot fix regulates the frequency at which the OfficeScan NT Listener service accesses the "¥Temp¥LogServer" folder to keep the number of write operations within the manageable range.

Issue 2: After upgrading to OfficeScan 11 Service Pack 1, the OfficeScan Master Service may not be able to start because the Trend Micro Active Update (AU) module cannot start successfully.

Solution 2: This hot fix allows users to enable the AU module to check certificates to help ensure that the module can start successfully.

Issue 3: While running a scan, the OfficeScan agent may unexpectedly launch the "TSCCensus.exe" process which is used for Smart Protection Network feedback. When this happens on the Microsoft(TM) Windows(TM) platform, Windows opens a command prompt to "C:¥WINDOWS¥TSCCensus.exe".

Solution 3: This hot fix allows users to prevent "TSCCensus.exe" from running while the OfficeScan agent is running a scan.

Hot Fix Build 4278.1

Issue: Users can prevent the OfficeScan server from generating firewall level logs through the following setting in the "ofcsan.ini" file and deploy this setting to all OfficeScan agents:

[Global Setting]
SkipFWLevelLog=1

OfficeScan agents will sync up the setting to the following registry key:

Path: HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ PC-cillinNTCorp¥Misc
Key: SkipFWLevelLog
Type: String
Value: 1

However, this key does not deploy correctly to OfficeScan agents that are installed on Microsoft(TM) Windows(TM) x64 platforms.

Solution: This hot fix ensures that users can prevent an OfficeScan server from generating firewall level logs through the OfficeScan server's "ofcscan.ini" file and deploy the setting to agents properly.

Hot Fix Build 4279/4784

Issue: When the OfficeScan client POP3 email scan is enabled, users sometimes receive an email with a blank subject, message and sender.

Solution: This hot fix resolves this issue.

Hot Fix Build 4280

Issue: The Behavior Monitoring Driver (Tmcomm.sys) of OfficeScan agents may have interoperability issues with some third-party system drivers which can trigger blue screen of death (BSoD).

Solution: This hot fix updates the Behavior Monitoring Driver to remove the interoperability issues and prevent BSoD.

Hot Fix Build 4281/4786

Enhancement: This hot fix prevents the sequence "000000000000" from triggering the "Japan-My Number Individual" identifier.

Hot Fix Build 4282

Issue: An issue related to the AEGIS module of the OfficeScan agent program may cause certain operating systems to stop responding.

Solution: This hot fix updates the Behavior Monitoring Service module to resolve the issue.

Hot Fix Build 4283/4797

Issue: An issue may prevent Trend Micro Control Manager(TM) from applying changes to the scan exclusion list of the OfficeScan agent.

Solution 1: This hot fix resolves the issue to ensure that Control Manager can successfully apply changes to the scan exclusion list of OfficeScan agents.

Issue: Sometimes, OfficeScan 11.0 Service Pack 1 agents may not be able to block access to a web site properly in computers running Microsoft(TM) Windows(TM) 7. This happens when the Web Reputation Service (WRS) is enabled and Suspicious Connection Service is disabled.

Solution 2: This hot fix updates the OfficeScan agent programs to resolve this issue on affected computers.

Hot Fix Build 4286

Issue: When an OfficeScan server uses an SQL Server as a database, the "DbServer.exe" process encounters a database exception error and stops unexpectedly, if it encounters a null value in the agent domain information.

Solution: This hot fix updates the SQL procedure in the OfficeScan server program to enable "DbServer.exe" to handle null values properly.

Hot Fix Build 4287

Issue: Sometimes, the OfficeScan database server stops unexpectedly while writing event logs on the database.

Solution: This hot fix ensures that the OfficeScan database server can write event logs on the database without issues.

Hot Fix Build 4288

Enhancement: This hot fix provides an option to enable the VSAPI feature on an OfficeScan server and to automatically deploy the setting to OfficeScan clients.

Hot Fix Build 4292

Issue 1: When the device control function for "NonStorage USB Device" is enabled, The OfficeScan Data Loss Prevention (TM) (DLP) module also blocks the SCSI Disk.

Solution 1: This hot fix ensures that The OfficeScan Data Loss Prevention Endpoint SDK 6.0 does not block the "USB LAN adapter" when the device control function for "NonStorage Usb Device" is enabled.

Issue 2: The OfficeScan Data Loss Prevention(TM) (DLP) module generates large temporary files during SMB transmission. These take up a large portion of disk space.

Solution 2: This hot fix prevents the OfficeScan DLP module from generating temporary files during SMB transmission.

Hot Fix Build 4295

Issue 1: An issue may prevent Trend Micro Control Manager(TM) from applying changes to the scan exclusion list of the OfficeScan agent.

Solution 1: This hot fix resolves the issue to ensure that Control Manager can successfully apply changes to the scan exclusion list of OfficeScan agents.

Issue 2: After users configure Trend Micro Data Loss Prevention(TM) (DLP) policies on the OfficeScan server console and deploy these policies to agents, the DLP policies are not applied correctly to OfficeScan agent computers.

Solution 2: This hot fix updates the OfficeScan agent program to ensure that DLP policies are applied to OfficeScan agent computers successfully.

Hot Fix Build 4296

Issue: When the database of the Trend Micro Local Web Classification Server (WRS) becomes corrupted while it is being opened, WRS fails to recover the database and causes succeeding updates to fail.

Solution: This hot fix manages the possible error that can occur while opening the WRS database. This hot fix enables WRS to rebuild the database when an error occurs while opening the database.

Hot Fix Build 4299

Enhancement: This hot fix allows users to configure OfficeScan to display the release date of the current Virus Pattern or Smart Scan Agent Pattern in the component version page of the OfficeScan agent console based on the scan mode.

Hot Fix Build 4300

Issue 1: When the Server Authentication feature is disabled, OfficeScan agents cannot upgrade the agent program from the Update Agent.

Solution 1: This hot fix ensures that the OfficeScan agent can upgrade from the Update Agent successfully when the Server Authentication feature is disabled.

Issue 2: Sometimes, the OfficeScan Master Service stops unexpectedly while the OfficeScan server retrieves policies from Trend Micro Control Manager(TM).

Solution 2: This hot fix ensures that the OfficeScan server can retrieve policies from Control Manager successfully.

Hot Fix Build 4301

Issue: When an OfficeScan server uses an SQL Server as a database, the "DbServer.exe" process encounters a database exception error and stops unexpectedly, if it encounters a null value in the agent domain information.

Solution: This hot fix updates the SQL procedure in the OfficeScan server program to enable "DbServer.exe" to handle null values properly.

Hot Fix Build 4302.u

Issue: Users who do not have administrator privileges cannot install an OfficeScan agent on the 64-bit version of Windows 10 using an MSI package created by the ClientPackager tool.

Solution: This hotfix ensures that users without administrator privileges can install the OfficeScan agent under the scenario described above.

Hot Fix Build 4304

Issue 1: OfficeScan Data Loss Prevention(TM)(DLP) takes a long time to copy files from Microsoft(TM) Outlook(TM) 2010 to a USB stick.

Solution 1: This hot fix ensures that users can copy files normally from Outlook 2010 to a USB stick.

Issue 2: OfficeScan Data Loss Prevention(TM)(DLP) unable to block sensitive file upload to Dropbox by using Google Chrome.

Solution 2: This hot fix ensures can block sensitive file upload to Dropbox by using Google Chrome.

Issue 3: When the OfficeScan Data Loss Prevention (DLP) module is run on Microsoft Windows 7 platforms, a blue screen error may occur.

Solution 3: This hot fix resolves the issue so that the DLP module in OfficeScan does not cause a blue screen error in Microsoft Windows 7.

Hot Fix Build 4305/4906

Issue: On Microsoft(TM) Windows(TM) 32/64-bit operating systems, the OfficeScan agent cannot be installed using an MSI package created by the ClientPackager tool if the cabinet file is larger than 300MB.

Solution: This hotfix allows users to adjust the threshold size of cabinet files that the ClientPackager tool generates to help ensure that the OfficeScan agent can be installed properly.

Hot Fix Build 4306

Enhancement: This hotfix enables users to globally deploy the Osprey module's "MaxHeaderCount" setting from the OfficeScan server to all OfficeScan clients. Setting this key to "0" can help ensure that users will be able to load websites normally on OfficeScan client computers.

Hot Fix Build 4307

Issue: The OfficeScan DLP module may not be able to block certain types of SD cards.

Solution: This hotfix ensures that when configured correctly, the OfficeScan DLP module can block SD cards.

Hot Fix Build 4308

Issue: When users add a program to the Trusted Program List and click "Save", the OfficeScan server console waits for the server to notify it if the operation was successful or if it has failed. If users click on the "Save" button multiple times while the server console is waiting for the response, the server console will pass redundant add-entry requests to the server which results in duplicate entries in the Trusted Programs List.

Solution: This hot fix prevents this issue by enabling the OfficeScan server console to temporarily disable operation buttons, "Add" and "Cancel" for example, in the "Trusted Program List" page and to automatically enable the buttons after it receives a response from the server.

Hot Fix Build 4310/4810

Issue: When users hide a drive through a group policy, the drive will still be visible in the folder tree on the manual scan page of the OfficeScan 11 agent console.

Solution: This hot fix ensures that the OfficeScan agent displays only the applicable drives in the folder tree on the manual scan page.

Hot Fix Build 4692

Issue: The information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan (Scan Now)" fields on the "Agent Management" page of the OfficeScan web console are not updated after a Manual Scan or a Scan Now task completes.

Solution: This hot fix updates some OfficeScan files to ensure that the information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan (Scan Now)" fields on the "Agent Management" page of the OfficeScan web console are updated promptly after each virus scan task.

Hot Fix Build 4693.1

Issue: The OfficeScan client cannot successful perform a manual scan on a remote drive that runs on a Microsoft(TM) Windows(TM) XP platform.

Solution: This hot fix ensures that the OfficeScan client successful performs a manual scan on a Microsoft Windows XP remote drive.

Hot Fix Build 4710

Issue: When users trigger the "Scan Now" feature of an OfficeScan agent to run a manual scan, some drives do not appear in the scan folder selection box.

Solution: This hot fix updates some OfficeScan files to ensure that the scan folder selection box displays all drives under the scenario described above.

Hot Fix Build 4712

Issue: OfficeScan clients that are installed on Microsoft(TM) Windows(TM) Server 2012 R2 with Domain Controller are displayed as "WindowsNT Platform Series" on the agent management tree. This happens because the Window API uses a stand-alone type to indicate the domain controller server and some OfficeScan server programs cannot handle this type.

Solution: This hot fix enables OfficeScan to handle domain controller server types so it can display the correct information on the agent management tree.

Enhancement: This hot fix ensures that OfficeScan displays Trend Micro Data Loss Prevention(TM) violation notification pop ups in the correct session by enabling it to check if the user name in the pop up window matches the login name for the current session before displaying the pop up.

Hot Fix Build 4714

Enhancement: This hot fix enables users to configure a Web Reputation policy for agents running Microsoft(TM) Windows(TM) Server 2003, Windows Server 2008, or Windows Server 2012 by selecting the root domain icon, specific domains, or specific agents in the "Agent Management" page of the OfficeScan web console.

Hot Fix Build 4727

Issue: If the OfficeScan server uses an SQL database, the contents of Scan Exclusion List (Directories) and Scan Exclusion List (Files) are removed when administrators select a domain and save the Scan Exclusion settings.

Solution: This hot fix resolves this issue so that the contents of Scan Exclusion List (Directories) and Scan Exclusion List (Files) are retained after performing the save operation.

Hot Fix Build 4732

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4751.1

Issue 1: After an OfficeScan 11 agent that was installed using an MSI package is upgraded to OfficeScan 11 Service Pack 1, the agent program cannot be uninstalled from the

Microsoft(TM) Windows(TM) "Control Panel > Programs and Features" page because it will not accept the correct password.

Solution: This hot fix updates the OfficeScan program to ensure that users will be able to uninstall OfficeScan 11 Service Pack 1 agents using the correct password through the Windows "Control Panel > Programs and Features" page.

Issue 2: Logon user names that contain Japanese characters cannot be displayed correctly in the client tree on the OfficeScan web console.

Solution: This hot fix ensures that logon user names that contain Japanese characters are displayed correctly in the client tree on the OfficeScan web console.

Hot Fix Build 4762

Issue: When users deploy an OfficeScan "Approved Programs" list under the Behavior Monitoring setting, it displays truncated path names. The path names may be truncated after the first "P" or "T" character.

Solution: This hot fix updates the OfficeScan program to ensure that the complete path names appear in the "Approved Programs" list of the Behavior Monitoring setting.

Hot Fix Build 4769

Issue: The "dsu_convert.exe" tool stops unexpectedly and triggers an error message when it encounters multibyte characters in the "DomainSetting.ini" file.

Solution: This hot fix resolves this issue by enabling the "dsu_convert.exe" tool to support multibyte characters.

Hot Fix Build 4771

Issue: The OfficeScan Master Service, "OfcService.exe", stops unexpectedly while managing OfficeScan tasks.

Solution: This hot fix updates the OfficeScan server files to resolve this issue.

Enhancement: This hot fix enables the OfficeScan 11.0 server to download the list of approved USB devices of the Device Control Settings from the Trend Micro Control Manager(TM) server and to deploy the list to OfficeScan agents.

The list of approved USB devices supports up to 18,000 devices.

Hot Fix Build 4780

Issue: OfficeScan Data Loss Prevention (DLP) blocks PDF files.

Solution: This hot fix updates the template and revises four regular expressions of the entity to solve the problem.

Hot Fix Build 4781

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4789

Issue: The OfficeScan client receives modified data during pattern updates which could be malware-related.

Solution: This hot fix ensures that all pattern files deployed to the OfficeScan client are verified before the pattern is incorporated into the client folder.

Hot Fix Build 4791

Enhancement: This hot fix enables Data Loss Prevention(DLP) Endpoint to avoid start up issues of guest hosts on Oracle(TM) VirtualBox(TM) when the DLP service has been started.

Hot Fix Build 4801

Issue: The OfficeScan client receives modified data during pattern updates which could be malware-related.

Solution: This hot fix ensures that all pattern files deployed to the OfficeScan client are verified before the pattern is incorporated into the client folder.

Hot Fix Build 4803

Issue: The result from an unmanaged endpoints query is not correct when using an SQL server as the OfficeScan database and the client numbers are large.

Solution: This hot fix ensures the query result of unmanaged endpoints is correct.

Hot Fix Build 4803

Issue: The OfficeScan Control Manager Agent process sometimes stops unexpectedly while receiving invalid log commands from the OfficeScan Master service.

Solution: This hot fix updates the OfficeScan server files to prevent the OfficeScan Master service from sending invalid commands to the OfficeScan Control Manager agent.

Hot Fix Build 4805

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4822

Issue: An issue prevents users from saving changes to the scan trigger settings of Real-time Scan on the OfficeScan client console.

Solution: This hot fix ensures that users can successfully edit and save changes in the scan trigger settings of Real-time Scan on the OfficeScan client console.

Hot Fix Build 4825

Issue: When an OfficeScan 10.6 Service Pack 3 agent is configured not to upload firewall logs, it may automatically start uploading these logs after restarting.

Solution: This hot fix ensures that OfficeScan clients upload firewall logs only when enabled to do so.

Hot Fix Build 4826

Issue 1: Users may receive several "Access Denied" notifications about CD drives even when they have not attempted to access any CD drive or USB device from protected computers.

Solution 1: This hotfix updates the AEGIS module to prevent the false alarms.

Issue 2: Certain programs may not work normally when the Unauthorized Change Management feature is enabled on OfficeScan client computers.

Solution 2: This hotfix updates the AEGIS module to solve the issue.

Hot Fix Build 4828

Issue: OfficeScan does not block ransomware set to a remote file server specified by a UNC path.

Solution: This hotfix enables OfficeScan to detect ransomware set to a remote file server specified by a UNC path.

Hot Fix Build 4830

Issue: On 32-bit OfficeScan clients running on 32-bit Microsoft(TM) Windows(TM) platforms, some file handles remain after OfficeScan runs a manual scan on a remote drive. This issue more commonly affects EMC storage devices.

Solution: This hotfix resolves this issue by enabling OfficeScan to use the same API set (VSAPI or AEGIS) for manual scans.

Hot Fix Build 4833

Issue 1: Launch application like Internet Explorer will cause OfficeScan Data Loss Prevention(TM)(DLP) Blue Screen of Death(BSoD) when Enhanced Mitigation Experience Toolkit(EMET) 5.5 is enabled.

Solution 1: This hot fix bypass the process injected by EMET to resolves the BSoD issue.

Issue 2: OfficeScan Data Loss Prevention(TM)(DLP) not blocked sensitive file uploading to Dropbox web by using Internet Explorer.

Solution 2: This hot fix provide support for Dropbox web upload based on new Dropbox version.

Hot Fix Build 4834.u

Issue: When the OfficeScan server has been upgraded from version 10.6 Service Pack 3 Patch 1.1 to version 11 Service Pack 1 Critical Patch 4150, users cannot upgrade OfficeScan clients to version 11 Service Pack 1 Critical Patch 4150 using an MSI installer package created by the Client Packager tool.

Solution: This hotfix ensures that users can upgrade OfficeScan clients to version 11 Service Pack 1 Critical Patch 4150 using the MSI installer package from the Client Packager tool.

Hot Fix Build 4835

Issue: On February 29, users encounter an internal error when generating certificates in OfficeScan using the following command:

CertificateManager.exe -c

This occurs because on February 29, OfficeScan automatically sets the certificate's end date to three years later which trigger the certificate creation API to return an error.

Solution: This hotfix enables the OfficeScan server to calculate the certificate's end time correctly on leap years.

Hot Fix Build 4836

Issue: An issue prevents the OfficeScan server from saving the AD grouping correctly if the AD domain hierarchy has child domains.

Solution: This hotfix resolves the issue to ensure that the OfficeScan server can save the AD grouping correctly.

Hot Fix Build 4837

Issue: Some OfficeScan clients disappear from the client list on the OfficeScan server console after users sort the clients on the list.

Solution: This hotfix resolves a logic issue in the database server to ensure that the users can sort the OfficeScan client list without issues.

Hot Fix Build 4838

Issue: On Microsoft(TM) Windows(TM) 32/64-bit operating systems, the OfficeScan agent cannot be installed using an MSI package created by the ClientPackager tool if the cabinet file is larger than 300MB.

Solution: This hotfix allows users to adjust the threshold size of cabinet files that the ClientPackager tool generates to help ensure that the OfficeScan agent can be installed properly.

Hot Fix Build 4840

Issue: After users successfully disable the Device Control settings for the Data Loss Prevention module of an OfficeScan client through the OfficeScan server console, the settings still appear as enabled on the client console.

Solution: This hotfix prevents the OfficeScan client console from displaying the Device Control settings page for its Data Loss Prevention module when these settings are disabled.

Hot Fix Build 4841

Issue: Disabling the "Enable virus/malware scan" option in an OfficeScan client disables Scan Now, however, Scan Now may still run after updates when the "Perform Scan Now after update (excluding roaming clients)" option is enabled.

Solution: This hot fix ensures that Scan Now cannot be triggered when the "Enable virus/malware scan" Scan Now option is disabled even when the "Perform Scan Now after update (excluding roaming clients)" option is enabled.

Hot Fix Build 4843

Issue: The OfficeScan server database did not sort agent results as expected.

Solution: This hotfix updates the OfficeScan server database so that agent results sort as expected.

Hot Fix Build 4849

Issue: On Microsoft(TM) Windows(TM) 32/64-bit operating systems, the OfficeScan agent cannot be installed using an MSI package created by the ClientPackager tool if the cabinet file is larger than 300MB.

Solution: This hotfix allows users to adjust the threshold size of cabinet files that the ClientPackager tool generates to help ensure that the OfficeScan agent can be installed properly.

Hot Fix Build 4854/4855

Issue: The Agent Packager does not properly include all required Visual C++ runtime libraries when creating an agent MSI installation package.

Solution: This hotfix updates the Agent Packager tool to properly include all required runtime libraries during the creation of an agent MSI installation package.

Hot Fix Build 4855

Issue: The ClientPackager tool generates large MSI installation packages when there is a large number of Memory Inspection Patterns persist on the OfficeScan server.

Solution: This hotfix updates the OfficeScan server program to help ensures that the ClientPackager tool creates MSI packages that are within the normal size range.

Hot Fix Build 4856

Issue: Sometimes, when OfficeScan agents upload logs to the server, a large volume of CGI calls may keep the web server and prevent the web console from responding promptly.

Solution: This hotfix updates the OfficeScan server and agent programs to improve the handling of CGI calls and help prevent performance issues on the web server.

Hot Fix Build 4857

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4857.1

Issue: The OfficeScan agent DLP module does not block users from sending out a new email message with a file attachment that contains sensitive information through Yahoo(TM) Mail in the Mozilla(TM) Firefox(TM) web browser.

Solution: This hotfix updates the OfficeScan agent DLP module to enable it to block users from attaching files that contain sensitive information to email messages.

Hot Fix Build 4858

Issue: When users attempt to register OfficeScan to a Trend Micro Control Manager(TM) server that communicates using Transport Layer Security (TLS) 1.2, the registration fails and users encounter an error on the Control Manager console.

Solution: This hot fix enables OfficeScan to support TLS 1.2. This ensures that it can register to a Control Manager server using this protocol.

Hot Fix Build 4865

Issue: If Integrated Smart Protection Server (iSPS) is not installed on an OfficeScan 11.0 Service Pack 1 with Critical Patch 4150 server, the URL for the default ActiveUpdate (AU) server will not be set in the AU.ini file. As a result, the Agent Packager Tool cannot properly update the crcz.ptn file when creating an agent MSI installation package.

Solution: This hotfix updates the OfficeScan 11.0 Service Pack 1 with Critical Patch 4150 agent files to prevent the issue.

Hot Fix Build 4872

Enhancement: This hot fix enables users to configure the OfficeScan server to notify agents to retrieve and apply configuration updates without waiting for a notification from the Update Agent.

Hot Fix Build 4873

Enhancement: This hotfix enables the DLP Endpoint SDK 6.0 module to support version 49.0.2623.110 of the Google(TM) Chrome(TM) web browser.

Hot Fix Build 4879

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4880

Issue: OfficeScan 11 SP1 Behavior Monitoring blocks a valid application.

Solution: This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to solve the issue.

Hot Fix Build 4882

Issue: OfficeScan Behavior Monitoring Ransomware Protection detects customer's developed software as malicious even after the software was added to the exception list.

Solution: This hotfix enhances the Behavior Monitoring exception list handling process to avoid this issue.

Hot Fix Build 4884

Enhancement: This hotfix enables OfficeScan clients to send malicious files that were detected and quarantined by the Behavior Monitoring Ransomware Protection feature to the OfficeScan server. This hotfix also ensures that each OfficeScan client keeps a back-up of these files with the original filenames in the client installation directory.

Hot Fix Build 4885

Issue: It may take a long time for users to log on to computers running on the Windows platform when the "Delay the RealTime Scan service from starting at startup" feature of the OfficeScan 11.0 Service Pack 1 agent program is enabled.

Solution: This hotfix updates the OfficeScan agent program to prevent the performance issue and ensure that users can log on to protected computers normally.

Hot Fix Build 4889/4902

Issue: The OfficeScan agent program may be vulnerable to potential unintended file access attacks.

Solution: This hotfix improves a checking mechanism in the OfficeScan agent program to protect it against unintended file access attacks.

Hot Fix Build 4890/4940.1

Issue: Several duplicate entries appear in the Behavior Monitoring Exclusion List.

Solution: This hotfix disables the "Save" button on the page immediately after users click on it.

Hot Fix Build 4896.1

Issue: Traffic from the Veeam Endpoint Backup program incorrectly triggers the OfficeScan agent DLP module.

Solution: This hotfix adds traffic sent by Veeam Endpoint Backup and all related executable files to the API hook and Network approved lists to enable the OfficeScan agent DLP module to skip these traffic.

Hot Fix Build 4896

Enhancement: This hotfix adds the following user privilege settings for Firewall Profiles configuration in OfficeScan 11.0 Service Pack 1:

- Allow users to change the security level
- Allow users to configure policy exceptions

Hot Fix Build 4901

Issue: Google Drive has switched networking protocols which prevents the DLP Endpoint SDK 6.0 agent from detecting violations related to the drive such as the upload of sensitive files to and from the drive.

Solution: The hotfix enables the DLP Endpoint SDK 6.0 agent to detect when a sensitive file is being to and from Google Drive.

Hot Fix Build 4902

Enhancement: This hotfix adds a way to configure OfficeScan clients to skip digital signature checking of OfficeScan client program files while downloading hotfix files and reloading the scan engine.

Hot Fix Build 4902.1

Issue: Users may not be able to uninstall non-English OfficeScan agent versions from computers running on the English version of the Windows platform.

Solution: This hotfix updates the OfficeScan agent program to ensure that users can uninstall non-English OfficeScan agent versions from computers running on the English version of the Windows platform normally.

Hot Fix Build 4906

Issue: The scan action information that appears in the Control Manager console does not match the information in OfficeScan logs.

Solution: This hotfix ensures that the OfficeScan server sends the correct scan action results to Control Manager so that the information in the Control Manager console matches the information on OfficeScan logs.

Hot Fix Build 4909/4940

Issue 1: The self-protection feature prevents OfficeScan 11.0 agents from deleting dump files.

Solution 1: This hotfix ensures that OfficeScan agents can successfully delete unnecessary OfficeScan client dump files immediately after restarting.

Issue 2: The OfficeScan Update Agent does not deploy the Suspicious Connection Settings to OfficeScan clients.

Solution 2: This hotfix ensures that the OfficeScan Update Agent deploys the Suspicious Connection Settings to OfficeScan clients.

Hot Fix Build 4912

Issue: The image path for the OfficeScan agent "OfficeScan Common Client Solution Framework" service contains a space that is not enclosed in double quotation marks. This creates a vulnerability.

Solution: This hot fix adds the missing double quotation marks to the image path of the "OfficeScan Common Client Solution Framework" service to resolve the vulnerability.

Hot Fix Build 4920

Issue: The scan action information that appears in the Control Manager console does not match the information in OfficeScan logs.

Solution: This hotfix ensures that the OfficeScan server sends the correct scan action results to Control Manager so that the information in the Control Manager console matches the information on OfficeScan logs.

Hot Fix Build 4921

Issue 1: Users cannot launch VMware ThinApp after enabling the DLP feature on protected computers.

Solution 1: This hotfix resolves an interoperability issue between the OfficeScan DLP feature and VMware ThinApp to ensure that the application works normally on protected computers.

Issue 2: The DLP module may falsely detect "CATIA" file contents in CAT files, for example, .CATDrawing, .CATPart, and .CATProduct files.

Solution 2: This hotfix prevents the false detections.

Hot Fix Build 4922

Issue: Installing OfficeScan 10.0 Service Pack 1 Patch 5 by web installation also installs ActiveX on the computer, however, ActiveX is not removed during client uninstallation. As a result, users encounter an error while installing OfficeScan 11 Service Pack 1 Critical Patch

4665 by web installation. This happens because the "WinNTchk.dll" for the ActiveX component cannot be updated when a previous version of the file exists in the installation directory. When this happens, the web installation fails.

Solution: This hotfix ensures that the OfficeScan server adds the version information of the "WinNTChk.cab" file when it triggers web installation.

Hot Fix Build 4925

Enhancement: This hot fix enables Data Loss Prevention(TM)(DLP) 6.0 to provide "-p" option to show parent's device information for device blockage.

Hot Fix Build 4926/4945

Issue: A handle leak issue that may occur while the OfficeScan server handles the "ofcserver.ini" file may corrupt the file.

Solution: This hotfix resolves the issue by ensuring that the OfficeScan server handles the INI properly.

Hot Fix Build 4928

Enhancement: This hotfix contains new versions of the "Trend Micro NSC Firefox Extension" and "Trend Micro Osprey Firefox Extension". These versions comply with the new security guidelines.

Hot Fix Build 4930

Issue 1: Users can add only up to 50 custom IP ranges in the IP range list of the Smart Protection Source.

Solution 1: This hotfix allows users to manually configure the maximum number of custom IP ranges in the IP range list of the Smart Protection Source.

Issue 2: After upgrading to OfficeScan 11 Service Pack 1, the digital signature cache may not work because OfficeScan agents do not build a local digital signature cache file for scanning files.

Solution 2: This hotfix resolves the issue by updating the OfficeScan agent program to enable OfficeScan agents to build a local digital signature cache file for scanning files.

Hot Fix Build 4934

Enhancement: This hotfix enables users to configure the OfficeScan server to notify OfficeScan agents to stop communicating with the census server while restarting.

Hot Fix Build 4937

Issue 1: The Trend Micro Common Client Solution Framework Service may become unresponsive when there is an interoperability issue between SHA256 certificates and an underlying 3rd-party SSL library.

Solution 1: This hot fix updates the related modules to resolve this issue.

Issue 2: The AutoPCC process may hang when installing the OfficeScan agent program.

Solution 2: This hot fix provides the following workaround which allows AutoPCC to launch successfully.

Hot Fix Build 4939

Issue: The OfficeScan DLP module may trigger a high CPU usage issue on Windows Server platforms with multiple logon sessions.

Solution: This hotfix enables users to configure the DLP module to wait for a specified time (in seconds) in between logon session information queries. Adjusting this time interval can prevent DLP from querying the logon session information frequently and prevent the high CPU usage issue.

Users need to manually add and configure the "monitor_agent_session_time" key on OfficeScan clients running on the Windows Server platform that provides multiple login service.

Hot Fix Build 4942

Enhancement: This hotfix enhances the OfficeScan folder write permission check before doing the SQL migration. End users should grant Windows domain users full control permissions to the OfficeScan server folder and include inheritable permissions from the parent of this object by local administrator or Active Directory (AD) build-in administrator.

Hot Fix Build 4946

Issue: A network isolated environment does not allow access to the Internet. Under this type of environment, the OfficeScan NT RealTime Scan service may cause OfficeScan agent computers to take a long time to copy or move .TIF files.

Solution: This hotfix improves the OfficeScan agent program to prevent this performance issue in network isolated environments.

Hot Fix Build 4947

Issue: The OfficeScan Master Service causes a high CPU usage issue when the Control Manager server sends a synchronization request of the OfficeScan agent information. This occurs when the "ClientInfoEnabled¡¨ registry value is zero for the OfficeScan Control Manager Agent.

Solution: This hotfix resolves the CPU usage issue by resetting the specic event when the "ClientInfoEnabled¡¨ registry value is zero preventing the repeated process loop.

Hot Fix Build 4948

Issue: Sometimes, the DLP module needs more time to retrieve IP addresses from host names when there is a large number of network connections.

Solution: This hotfix resolves the performance issue by allowing DLP to skip IP address retrieval if the FQDN is in the global approved list and the user is currently using FQDN to connect to remote servers.

Hot Fix Build 4950

Issue: The OfficeScan exclusion list does not work on mount points; drives that are mapped as folders to an existing file system.

Solution: This hotfix ensures that OfficeScan clients receive the complete list of approved devices to ensure that the exclusion list works normally.

Hot Fix Build 4954

Issue 1: The scan action information that appears in the Control Manager console does not match the information in OfficeScan logs.

Solution 1: This hotfix ensures that the OfficeScan server sends the correct scan action results to Control Manager so that the information in the Control Manager console matches the information on OfficeScan logs.

Issue 2: When an OfficeScan client detects malware, the corresponding pop-up window indicates that the instance has been "resolved" instead of "found". This occurs even when the OfficeScan client cannot perform the required action on the malware.

Solution 2: This hotfix ensures that the pop-up window correctly indicates that the malware has been "found".

Hot Fix Build 4954.1

Issue: When an OfficeScan client detects malware, the corresponding pop-up window indicates that the instance has been "resolved" instead of "detected". This occurs even when the OfficeScan client cannot perform the required action on the malware.

Solution: This hotfix ensures that the pop-up window correctly indicates that the malware has been "detected".

Hot Fix Build 4956

Issue: Sometimes, users cannot remove the OfficeScan DLP policy if the policy is assigned to an OfficeScan agent that does not exist.

Solution: This hotfix ensures that users can remove the OfficeScan DLP policy without issues.

Hot Fix Build 4958

Issue: The Windows shortcut menu item for Manual Scans in OfficeScan agents does not work when the "Do not allow users to access the OfficeScan agent console from the system tray or Windows Start menu" option in the "Agent Management > Settings > Privileges and Other Settings > Other Settings" page is enabled.

Solution: This hotfix ensures that the Manual Scan shortcut menu item works normally.

Hot Fix Build 4960

Issue: The "Firewall Setting" option still appears on the "Agent management > Setting > Privileges and Other Settings" page when "Firewall for endpoints" is disabled on the “Product License” page in the web console.

Solution: This hotfix enables OfficeScan to hide the "Firewall Setting" option automatically when "Firewall for endpoints" is disabled on the “Product License” page in the web console.

Hot Fix Build 4960.1

Enhancement: This hot fix enables the OfficeScan server to check if a unique identifier (UID) of a client exists in the database and notifies the client machine to register again if it has no record of the client's UID.

Hot Fix Build 4961

Issue 1: The OfficeScan server sends configuration change notifications to OfficeScan agents twice.

Solution 1: This hotfix ensures that the OfficeScan server sends only one notification for each set of configuration changes to OfficeScan agents.

Issue 2: The OfficeScan agent displays the short detection name on the Virus/Malware Logs.

Solution 2: This hotfix ensures that the OfficeScan agent displays the long detection name on the Virus/Malware Logs.

Hot Fix Build 4961.1

Issue: On the Agent Management web page of OfficeScan server console, the Advanced Search task may take more than one (1) minute before timing out without displaying the search results.

Solution: This hotfix extends the timeout value to ten (10) minutes, which allows the OfficeScan server to display the results of the Advanced Search results successfully.

Hot Fix Build 4962

Issue: A mismatch between the encode and decode calling mechanism prevents OfficeScan from syncing up with the Active Directory server.

Solution: This hot fix resolves the call mismatch issue so OfficeScan can sync up with the Active Directory server successfully.

Hot Fix Build 4977

Issue: There is an interoperability issue between the TMWFP driver and tmeevw service.

Solution: This hotfix removes an unused call out to resolve the interoperability issue.

Hot Fix Build 6077

Enhancement: This hotfix enables DLP Endpoint SDK 6.0 to support Chrome 51.0.2704.84m with QUIC enabled.

Hot Fix Build 6082

Issue: A handle leak issue that may occur while the OfficeScan server handles the "ofcserver.ini" file may corrupt the file.

Solution: This hotfix resolves the issue by ensuring that the OfficeScan server handles the INI properly.

Enhancements from hot fixes for OSCE 10.6 SP3

Hot Fix Build 5769.u

Enhancement: Third-party Product Uninstallation - The OfficeScan installation program now automatically removes the following products before installing the OfficeScan client:

- The Traditional Chinese versions of the following third-party products with the Traditional Chinese version of OfficeScan:
    - ESET NOD32 Endpoint Antivirus x86/x64 5.0.2228.1
    - ESET NOD32 File Security x86/x64 4.5.12015.3

Enhancements from hot fixes for OSCE 11.0

Hot Fix Build 1795.u, 1801.u, 1802.u, 1811.u, 1831.u, 1848.u, 1849.u, 1858.u, 1864.u, 1869.u, 1895.u, 1901.u, 1921.u, 1932.u, 2033.u, 2034.u

Enhancement: Third-party Product Uninstallation - The OfficeScan installation program now automatically removes the following products before installing the OfficeScan client:

- The English versions of the following third-party products with the English version of OfficeScan:
    - ESET Endpoint Antivirus 5.0.2229.1
    - Kaspersky Endpoint Security 8 for Windows 8.1.0.646
    - Kaspersky Endpoint Security 10 for Windows 10.2.1.23
    - Kaspersky Endpoint Security 10 for Windows 10.2.2.10535
    - Kaspersky Endpoint Security Center Network Agent 10.1.249
    - McAfee VirusScan Enterprise 8.7.00003
    - McAfee Agent 4.5.0.1852
    - McAfee Agent 4.5.0.1499
    - McAfee VirusScan Enterprise 8.8.0.1247 (x86/x64)
    - McAfee Agent 4.8.0.887 (x86/x64)
    - Sophos Patch Agent 1.0.303.0 (x86/x64)
    - Sophos Client Firewall 2.9.0
    - Sophos Anti-Virus 10.0.5
    - Sophos Anti-Virus 10.3.7 (x86/x64)
    - Sophos Remote Management System 3.4.0
    - Sophos Remote Management System 3.4.1 (x64)
    - Sophos Remote Management System 3.2.0 (x64)
    - Sophos Technical Support 10.0.5 (X64)
    - Sophos Auto Update 3.1.1.8 (x86/x64)
    - Sophos Auto Update 4.1.0.273 (x86/x64)
    - Symantec Endpoint Protection 12.1.1.1000.157
    - Symantec Endpoint Protection 12.1.617.4971 (x86/x64)
    - Symantec Endpoint Protection 12.1.2015.2015 (x86/x64)

    - Symantec Endpoint Protection 12.1.6168.6000 (x86/x64)
- The Traditional Chinese versions of the following third-party products with the Traditional Chinese version of OfficeScan:
    - Symantec Endpoint Protection 12.1.3001.165 (x86/x64)
- The Japanese versions of the following third-party products with the Japanese version of OfficeScan:
    - Symantec Endpoint Protection 12.1.4100.4126 (x86/x64)
    - Symantec Endpoint Protection 12.1.4013.4013 (x86/x64)
- The German versions of the following third-party products with the Traditional Chinese version of OfficeScan:
    - Symantec Endpoint Protection 12.1.5337.5000 (x86/x64)

Enhancements from hot fixes for OSCE 11.0 SP1

Hot Fix Build 3011.u, 3026.u, 3027.u, 3031.u, 3038.u, 3045.u, 3066.u, 3610.u

Enhancement: Third-party Product Uninstallation

The OfficeScan installation program now automatically removes the English versions of the following third-party products with the English version of OfficeScan before installing the OfficeScan client:

- Symantec(TM) Endpoint Protection 12.1.3001.165
- Symantec(TM) Endpoint Protection 12.1.3001.165 x64
- Symantec(TM) Endpoint Protection 12.1.5337.5000 x64
- Symantec(TM) Endpoint Protection 12.1.4100.4126 x64 French version
- Sophos Client Firewall 10.3.13 x86/x64
- Sophos Anti-Virus 10.3.13 x86/x64
- Sophos Remote Management System 10.3.13 x86/x64
- Sophos AutoUpdate 10.3.13 x86/x64
- Sophos Patch Agent 10.3.13 x86/x64
- McAfee Endpoint Encryption 7.0.3.413
- Kaspersky Endpoint Security 10.2.2.10535 (x86/x64)
- ESET Remote Administrator Agent 6.1.365.0 x86/x64
- ESET Remote Administrator Agent 6.1.444.0 x86/x64