Hot Fixes

Below are the issues resolved by the hot fixes in OSCE 11.0:

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.
Hotfix_1626.1

**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.

Hotfix_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.

Hotfix_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.

Hotfix_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 through 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.

Hotfix_1633

**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.

Hotfix_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".

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_1747

**Issue:** On OfficeScan clients, users cannot successfully install the third party software Sentinel License Development Kit (LDK) Runtime.

**Solution:** This hot fix updates the OfficeScan clients which prevent the installation of Sentinel LDK Runtime.

Hotfix_1747.1

**Issue:** When users access the OfficeScan web console in Microsoft(TM) Internet Explorer(TM) 8 and input Japanese characters while creating Trend Micro Data Loss Prevention(TM) (DLP) rules, identifiers or policy, the Japanese characters disappear after users save the settings.

**Solution:** This hot fix ensures that Japanese characters are displayed normally on the OfficeScan web console in Internet Explorer 8.

Hotfix_1748

**Issue:** When you upgrade from an older OfficeScan client version installed using an MSI package, to OfficeScan 11 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 stores the uninstallation password in a different location.

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

Hotfix_1763

**Issue:** DbServer.exe" may stop unexpectedly, cause a high CPU usage issue, or corrupt data.

**Solution:** This hot fix updates the OfficeScan files to add additional error-handling mechanisms to "DbServer.exe"

Hotfix_1767

**Issue 1:** This hot fix enables OfficeScan Data Loss Prevention(TM) Endpoint SDK to support the ability to block mobile devices on computers (for example, Apple(TM) iPhone 6 or iPhone 6 Plus).

**Solution 1:** This hot fix ensures that the Device Control feature can properly block
mobile devices.

**Issue 2:** The recipient information for email messages sent from Hotmail or Gmail may not appear in violation logs.

**Solution 2:** This hot fix ensures that the correct recipient information appear in violation logs.

Hotfix_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.

Hotfix_1773

**Issue:** If some fully-qualified domain names (FQDNs) in the approved list of programs of Data Loss Prevention Endpoint SDK are unavailable, it will take more time to resolve the DNS of applications and some applications may eventually time-out.

**Solution:** This hot fix resolves the issue by improving the mechanism for resolving FQDNs and IPs in Data Loss Prevention Endpoint SDK 6.0.1253.

Hotfix_1779

**Issue:** Users that do not have administrator privileges can switch to an administrator role.

**Solution:** This hot fix ensures that users that do not have administrator privileges cannot change user roles.

Hotfix_1781

**Issue:** An initialization issue prevents the OfficeScan Master Service from starting successfully after the OfficeScan server computer restarts.

**Solution:** This hot fix updates the OfficeScan server program file to enhance the OfficeScan Master Service initialization procedure and ensure that the service can start successfully after the OfficeScan server computer restarts.

Hotfix_1785

**Issue:** The OfficeScan server may generate duplicate domains on the "Agent Management" page of the OfficeScan web console if it cannot connect to the SQL
**Solution**: This hot fix prevents the OfficeScan server from generating duplicate domains on the "Agent Management" page.

**Hotfix_1789**

**Issue**: The shutdown time information in the "Last Shutdown" column on the "Agent Management" page of the OfficeScan web console are not updated when OfficeScan Agents are shut down through the Microsoft(TM) Windows(TM) platform.

**Solution**: This hot fix improves the job order of OfficeScan Agents, to ensure that the shutdown time information in the "Last Shutdown" column are updated promptly after OfficeScan Agents are shut down through Windows.

**Hotfix_1789.1**

**Issue**: In non-English OfficeScan versions, an error message appears when users run the SvrSvcSetup.exe tool using the "svrsvcsetup-enablessl" command.

**Solution**: This hot fix enables OfficeScan servers to write the corresponding registry keys directly when users make changes to the settings using SvrSvcSetup.exe tool commands. This helps ensure that the tool works normally.

**Hotfix_1790**

**Issue**: OfficeScan clients may not be able to upload some virus logs to the OfficeScan server.

**Solution**: This hot fix extends the file path buffer to ensure that OfficeScan clients can successfully upload virus logs to the OfficeScan server.

**Hotfix_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.
Hotfix_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.

Hotfix_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.

Hotfix_1808

**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.

Hotfix_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.

Hotfix_1811

**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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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 Callbacks 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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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".

Hotfix_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.

Hotfix_1865

**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.

Hotfix_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.

Hotfix_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.
Hotfix_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.

Hotfix_1886

**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.

Hotfix_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.

Hotfix_1912

**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.

Hotfix_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. Note: The unnecessary folder delete action will be triggered in the next successful update event. After the HF installation, please hold on until the next OfficeScan server update.
Hotfix_1914

**Issue:** The OfficeScan client cannot successfully 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 successfully performs a manual scan on a Microsoft Windows XP remote drive.

Hotfix_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 3:** This hot fix ensures that OfficeScan can effectively block users from uploading sensitive files to Gmail.

Hotfix_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.

Hotfix_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.
Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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 OfficeScan agents on the root domain.

Hotfix_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.
Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.
Hotfix_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.

Hotfix_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.

Hotfix_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".

Hotfix_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.

Hotfix_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.

Hotfix_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.

**Hotfix_1990**  
**Issue**: The OfficeScan server on-line help web page, ウイルスバスター Corp. クライアントプログラムのアップグレード, displayed in English.  
**Solution**: This hot fix updates the web page HTML file in Japanese to correct the issue.

**Hotfix_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.

**Hotfix_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.

**Hotfix_1998**  
**Issue**: Temp files that DLP module is using fill up disk space.  
**Solution**: This hot fix resolves the disk space usage issue.

**Hotfix_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.

**Hotfix_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.

Hotfix_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 standalone 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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_2030

**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.

Hotfix_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.

Hotfix_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.

Below are the issues resolved by the hot fixes in OSCE 11.0 SP1:

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_3015

**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".

Hotfix_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.

Hotfix_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.

Hotfix_3018

**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.

Hotfix_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.

Hotfix_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.

Hotfix_3029
**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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_3050**  
**Issue:** 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:** This hot fix updates the related modules to resolve this issue.

**Hotfix_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.

**Hotfix_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.
Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.
Hotfix_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.

---

Hotfix_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.

---

Hotfix_3066

**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.

**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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_3080

**Issue:** In some region, OfficeScan does not display the correct time format in the OfficeScan client console.

**Solution:** This hot fix resolves the time format issue.

Hotfix_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.

Hotfix_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.

*Hotfix_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.

*Hotfix_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.

*Hotfix_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.

*Hotfix_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.

*Hotfix_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.

**Hotfix_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.

**Hotfix_3090**

**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.

**Hotfix_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.

**Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_3613**  
**Issue:** The OfficeScan agent's NtrtScan.exe process crashes when it calls Data Loss Prevention's (DLP) TmDlpGetCurrentDiscVersion function.  
**Solution:** This hot fix updates the DLP module of the OfficeScan agent which validates the pointer before accessing its method.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_3649

**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.
Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_3681

**Issue 1:** The OfficeScan "cgiShowClientAdm.exe" and "cgiShowServerAdm.exe" processes are vulnerable to XSS.

**Solution 1:** 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.

**Issue 2:** Domain names that contain garbled characters cannot be displayed correctly in the client tree on the OfficeScan web console.

**Solution 2:** 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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_3700  
**Issue:** The OfficeScan agent displays the short detection name on the Virus/Malware Logs.  
**Solution:** This hotfix ensures that the OfficeScan agent displays the long detection name on the Virus/Malware Logs.

Hotfix_3704  
**Issue:** When the OfficeScan server receives multiple policies from a Control Manager 6.0 server, it applies only the first policy.  
**Solution:** This hotfix updates the OfficeScan program to ensure that the OfficeScan server can apply multiple policies from a Control Manager 6.0 server.

Below are the issues resolved by the hot fixes in OSCE 11.0 SP1 CP4150:

Hotfix_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.
Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_4177**

**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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

Hotfix_4187

**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.

Hotfix_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.

Hotfix_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.

Hotfix_4191

**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.

Hotfix_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.

**Hotfix_4201**

**Issue:** The Data Loss Prevention rule "UK: RD&E Hospital 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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_4204**

**Issue:** An OfficeScan agent that cannot connect to the OfficeScan server during startup will not be able to trigger scheduled updates.

**Solution:** This hot fix updates the OfficeScan 11.0 server and agent files to ensure that agents can still trigger scheduled updates when these agents cannot connect to OfficeScan server during startup.

**Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_4210

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.

Hotfix_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.

Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_4213.1**

**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.

**Hotfix_4215**

**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.

Hotfix_4216

**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.

Hotfix_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.

Hotfix_4218

**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.

Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_4227**

**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".

**Hotfix_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.

**Hotfix_4229**

**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.
Hotfix_4231

**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 through 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.

Hotfix_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.

Hotfix_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.

Hotfix_4237.1

**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.
Hotfix_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.

Hotfix_4239
**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.

Hotfix_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.

Hotfix_4241
**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.

Hotfix_4242
**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.

Hotfix_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.
**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.

**Hotfix_4245**

**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.

**Hotfix_4246**

**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.

**Hotfix_4247**

**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.

**Hotfix_4252**

**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 (*.xlsx) 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.

Hotfix_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.

Hotfix_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.

Hotfix_4256

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.

Hotfix_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.

Hotfix_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 2**: 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.

Hotfix_4269

**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.

Hotfix_4270

**Issue**: In the "Device Control Settings" page for USB storage approved devices of the OfficeScan web console, users cannot create an approved list that contains the number sign (#) in the USB serial number.

**Solution**: This hot fix ensures that users can create an approved list that contains the number sign (#) in the USB serial number of the OfficeScan web console.

Hotfix_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.

Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_4278**

**Issue 1**: The OfficeScan NT Listener service accesses the "<OSCEClientInstallDir>\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 "<OSCEClientInstallDir>\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.

**Procedure 2:** To enable the AU module to check certificates:

**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.

Hotfix_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 "ofcsan.ini" file and deploy the setting to agents properly.

Hotfix_4279

**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.

Hotfix_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.

**Hotfix_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.

**Hotfix_4283**

**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**: 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.

**Hotfix_4286.1**

**Issue**: When users access the OfficeScan web console in Microsoft(TM) Internet Explorer(TM) 8 and input Japanese characters while creating Trend Micro Data Loss Prevention(TM) (DLP) rules,identifier or policy, the Japanese characters disappear after users save the settings.

**Solution**: This hot fix ensures that Japanese characters are displayed normally on the OfficeScan web console in Internet Explorer 8. Note: After applying this hot fix, you need to recreate all previously-added DLP templates/identifier/policy to ensure that the solution from this hot fix works on these templates.

**Hotfix_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.

**Hotfix_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.

Hotfix_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**: 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.

**Issue 3**: Sometimes, the OfficeScan database server stops unexpectedly while writing event logs on the database.

**Solution 3**: This hot fix ensures that the OfficeScan database server can write event logs on the database without issues.

**Issue 4**: 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 4**: This hot fix updates the OfficeScan agent program to ensure that DLP policies are applied to OfficeScan agent computers successfully.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_4302

**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.

Hotfix_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.

Hotfix_4305

**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.

**Hotfix_4307**

**Issue 1:** In protected computers, Google Chrome 48.0.2564.10 stops unexpectedly when users print documents or webpages. This occurs because the OfficeScan Data Loss Prevention(TM) (DLP) module cannot block the QUIC network protocol in this Google Chrome 48.0.2564.10.

**Solution 1:** This hotfix enables the OfficeScan DLP module to block QUIC in Google Chrome 48.0.2564.10 to ensure that users can print webpages and documents without issues.

**Issue 2:** The OfficeScan DLP module may not be able to block certain types of SD cards.

**Solution 2:** This hotfix ensures that when configured correctly, the OfficeScan DLP module can block SD cards.

**Hotfix_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.

**Hotfix_4310**

**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.

**Hotfix_4692**

**Issue:** The information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan
"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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_4698**

**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.

**Hotfix_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.
Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_4727

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

**Solution:** This hot fix ensures that the contents of the Scan Exclusion List (Directories) and Scan Exclusion List (Files) do not change after administrators save the Scan Exclusion settings.

Hotfix_4733

Only JP has issue.

Hotfix_4733.1

**Issue 1:** The information in the "Last Virus Scan (Manual Scan)" and "Last Virus Scan
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 through 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.

Hotfix_4748

**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.

Hotfix_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.

Hotfix_4751.1

**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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_4757  
**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".

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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: 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 (*.xlsx) because the DLP function does not extract the contents of the files correctly.
Solution: This hot fix ensures that DLP can extract the files correctly and block sensitive content such as Microsoft Excel workbooks.

Hotfix_4766

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.
Hotfix_4768
**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.

Hotfix_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.

Hotfix_4771
**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.

Hotfix_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.

Hotfix_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.

Hotfix_4782
**Issue:** In the "Device Control Settings" page for USB storage approved devices of the OfficeScan web console, users cannot create an approved list that contains the number sign (#) in the USB serial number.
**Solution:** This hot fix ensures that users can create an approved list that contains the number sign (#) in the USB serial number of the OfficeScan web console.

Hotfix_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.

Hotfix_4785.1

**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.

Hotfix_4787

**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.

Hotfix_4788

**Issue:** The OfficeScan NT Listener service accesses the ":<OSCEClientInstallDir>\Temp\LogServer" folder frequently which triggers a large number of write operations on the local disk.

**Solution:** This hot fix regulates the frequency at which the OfficeScan NT Listener service accesses the ":<OSCEClientInstallDir>\Temp\LogServer" folder to keep the number of write operations within the manageable range.

Hotfix_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.
Hotfix_4791

**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.

Hotfix_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.

Hotfix_4794

**Issue:** When users access the OfficeScan web console in Microsoft(TM) Internet Explorer(TM) 8 and input Japanese characters while creating Trend Micro Data Loss Prevention(TM) (DLP) rules, identifier or policy, the Japanese characters disappear after users save the settings.

**Solution:** This hot fix ensures that Japanese characters are displayed normally on the OfficeScan web console in Internet Explorer 8.

**Note:** After applying this hot fix, you need to recreate all previously-added DLP templates/identifier/policy to ensure that the solution from this hot fix works on these templates.

Hotfix_4797

**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:** 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.

**Issue 3**: Sometimes, the OfficeScan database server stops unexpectedly while writing event logs on the database.

**Solution 3**: This hot fix ensures that the OfficeScan database server can write event logs on the database without issues.

**Issue 4**: After users configure Trend Micro Data Loss Prevention (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 4**: This hot fix updates the OfficeScan agent program to ensure that DLP policies are applied to OfficeScan agent computers successfully.

---

**Hotfix_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.

---

**Hotfix_4803**

**Issue 1**: 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 1**: This hot fix allows users to enable the AU module to check certificates to help ensure that the module can start successfully.

**Issue 2**: Logon user names that contain Chinese characters cannot be displayed correctly in the client tree on the OfficeScan web console.

**Solution 2**: This hot fix ensures that logon user names that contain Chinese characters are displayed correctly in the client tree on the OfficeScan web console.

**Issue 3**: The OfficeScan Control Manager Agent process sometimes stops unexpectedly while receiving invalid log commands from the OfficeScan Master service.

**Solution 3**: This hot fix updates the OfficeScan server files to prevent the OfficeScan Master service from sending invalid commands to the OfficeScan Control Manager agent.

**Issue 4**: The OfficeScan client receives modified data during pattern updates which could be malware-related.

**Solution 4**: This hot fix ensures that all pattern files deployed to the OfficeScan client are verified before the pattern is incorporated into the client folder.

---

**Hotfix_4805**
**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.

---

**Hotfix_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.

---

**Hotfix_4822**

**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:** 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 2:** 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.

---

**Hotfix_4824**

**Issue:** The "Initiate Unloading" option on the "Agent > Agent Management > Agent Uninstallation" screen of the Japanese version of the OfficeScan 11.0 server console is incorrectly labeled as "Initial Uploading".

**Solution:** This hotfix corrects the label of the "Initiate Unloading" option on the "Agent > Agent Management > Agent Uninstallation" page of the OfficeScan server console.

---

**Hotfix_4825**

**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.

---

**Hotfix_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:** 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 2:** This hot fix ensures that the OfficeScan Browser Exploit **Solution** feature works well with Internet Explorer.

**Issue 3:** Users are unable to execute any executables from network shares when the Unauthorized Change Management feature is enabled on OfficeScan client computers.

**Solution 3:** This hotfix updates the AEGIS module to solve the issue.

**Issue 4:** Certain programs may not work normally when the Unauthorized Change Management feature is enabled on OfficeScan client computers.

**Solution 4:** This hotfix updates the AEGIS module to solve the issue.

Hotfix_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.

Hotfix_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.

Hotfix_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
Hotfix_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.

Hotfix_4835
Issue: On February 29, users encounter an internal error when generating certificates in OfficeScan using the following command: CertificateManager.exe -c <backup password> 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.

Hotfix_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.

Hotfix_4836.1
Issue: On Microsoft(TM) Windows(TM) 64-bit operating systems, the OfficeScan agent cannot be installed using an MSI package created by the Client Packager tool if the cabinet file is larger than 300MB.
Solution: This hotfix allows users to adjust the threshold size of cabinet files that the Client Packager tool generates to help ensure that the OfficeScan agent can be installed properly.

Hotfix_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.
Hotfix_4838  
**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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_4849  
**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.

Hotfix_4854
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.

Hotfix_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 ensure that the ClientPackager tool creates MSI packages that are within the normal size range.

Hotfix_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.

Hotfix_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.

Hotfix_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 hotfix enables OfficeScan to support TLS 1.2. This ensures that it can register to a Control Manager server using this protocol.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_4889
**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.

Hotfix_4890
**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.
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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_4909

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.

Hotfix_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 hotfix adds the missing double quotation marks to the image path of the "OfficeScan Common Client Solution Framework" service to resolve the vulnerability.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_4926

**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
Hotfix_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.

---

Hotfix_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 hotfix updates the related modules to resolve this issue.

**Issue 2:** The AutoPCC process may hang when installing the OfficeScan agent program.

**Solution 2:** This hotfix provides the following workaround which allows AutoPCC to launch successfully.

---

Hotfix_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.

---

Hotfix_4940

**Issue:** The self-protection feature prevents OfficeScan 11.0 agents from deleting dump files.

**Solution:** This hotfix ensures that OfficeScan agents can successfully delete unnecessary OfficeScan client dump files immediately after restarting.
Hotfix_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.

Hotfix_4942

**Issue:** When using the Microsoft(TM) Windows domain user account to migrate an OfficeScan database from codebase to an SQL database, a "conhost.exe" application error might occur while updating the SQL schema.

**Solution:** This hotfix uses another method when handling the SQL schema update instead of using the Windows application program interface (API), which resolves this issue.

Hotfix_4943

**Issue:** Sometimes, a race issue related to the Virus Scan Engine and RealTime Scan service causes the OfficeScan agent computer to start slowly.

**Solution:** This hotfix enables OfficeScan agents to wait until the RealTime Scan service has started successfully before starting the Virus Scan Engine.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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".

Hotfix_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".

Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

Hotfix_4965

**Issue**: OfficeScan agent reports its status of antivirus to Windows Security Center (WSC) when the system starts. After restarting, the WSC sometimes displays that some of the OfficeScan components are not up-to-date.

**Solution**: This hotfix improves the speed in which the OfficeScan agent program reports its status to WSC.

Hotfix_4974

**Issue**: The "Last update" information shown on the OfficeScan agent console may cause confusion to users.

**Solution**: This hotfix updates the OfficeScan agent program to display the "Last update" information on the OfficeScan agent console in the same way as OfficeScan displays the "Last update" information on "Smart Scan Agent Pattern".

Hotfix_4976

**Issue**: Active Directory does not allow some special characters as Active Directory passwords.

**Solution**: This hotfix ensures that Active Directory can allow special characters as Active Directory passwords.

Hotfix_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.

Hotfix_4980

There is no issue in this hotfix.

**Issue**: This issue is caused by Trend Micro Local Web Classification Server file had been copied successfully, but the return is 9009.

**Solution**: This hotfix resolves this issue.

Hotfix_4983

**Issue**: Access Document Control (ADC) cannot detect files that run from the network drive.

**Solution**: This hotfix ensures that the ADC detection can successfully work on the network drive.
Hotfix_4986

**Issue:** Users encounter some unexpected issues in the OfficeScan client wherein the OfficeScan client queries the database even though there is no specific entry yet from the OfficeScan client to the database.

**Solution:** This hotfix updates the OfficeScan server by preventing queries from accessing the database before the client entry is ready.

Hotfix_4992

**Issue:** The listDeviceInfo tool cannot display any information about a special USB device if its device information is not in the usual format.

**Solution:** This hotfix updates the "listDeviceInfo.exe" tool to enable it to display information about USB devices when the device information is not in the usual format.

Hotfix_4993

**Issue:** When using the "Sort Agent" option to group OfficeScan agents based on the Active Directory structure, an unexpected domain structure is created on the Agent Management screen.

**Solution:** This hotfix updates the OfficeScan server to display the correct Active Directory domain structure on the Agent Management screen after sorting agents based on Active Directory.

Hotfix_4995

**Issue:** An arithmetic overflow error occurs and triggers the following Microsoft(TM) Windows(TM) application even log: "Arithmetic overflow error converting expression to data type int."

**Solution:** This hotfix updates the OfficeScan server database process (dbserver.exe) to reverse the order of parameters and prevent the arithmetic overflow event.

Hotfix_4996

**Issue:** When users run the client packager tool in the CLI to create client installation packages, they have no way to specify a domain where all freshly-installed clients should belong to.

**Solution:** This hotfix updates the client packager tool to enable users to specify a domain for freshly-installed clients using the "/domain" parameter when creating client installation packages through the CLI.

Hotfix_4999
**Issue**: Sometimes, an issue related to JSON data prevents the OfficeScan web console from displaying the contents of the DLP setting page. When this happens, users cannot deploy the DLP settings to clients.

**Solution**: This hotfix modifies a FlushJson function to resolve the issue and help ensure that the DLP setting page displays completely and users can deploy the DLP settings to clients.

**Hotfix_5002**

**Issue**: The following services provide robust protection but their monitoring mechanisms can strain system resources, especially on Windows server platforms:
- Unauthorized Change Prevention Service
- Suspicious Connection Service
- Advanced Protection Service
For this reason, these services are disabled by default on Windows Server 2003, 2008, and 2012.

**Solution**: This hotfix allows users to enable the services above by default on a freshly installed OfficeScan agent on the Windows Server platform.

**Hotfix_5003**

**Issue**: The OfficeScan 11.0 Service Pack 1 Behavior Monitoring feature blocks a valid program.

**Solution**: This hotfix updates the OfficeScan Behavior Monitoring Local Pattern to ensure that it blocks the correct programs.

**Hotfix_5008**

**Issue 1**: OfficeScan Data Loss Prevention (DLP) is unable to block the CD/DVD burning function of explorer.exe in "USB flash drive" mode.

**Solution 1**: The hot fix resolves the DLP blocking issue.

**Issue 2**: Data Loss Prevention only generates a maximum of 200 violation logs even if users burn more than 200 files (with violations) using the CD/DVD player function of explorer.exe.

**Solution 2**: The hot fix resolves the issue by enlarging the queue size to 100,000.

**Hotfix_5009**

**Issue 1**: Access Document Control (ADC) cannot detect files that run from the network drive.

**Solution 1**: This hotfix ensures that the ADC detection can successfully work on the network drive.

**Issue 2**: Duplicate DLP violation logs are uploaded to the OfficeScan server at five
minute intervals when the DLP Violation Log database file is corrupted.

Solution 2: This hotfix updates the OfficeScan agent program to ensure that it uploads DLP violation logs to the OfficeScan server normally.

Hotfix_5014
Issue: When the OfficeScan server receives multiple policies from a Control Manager 6.0 server, it applies only the first policy.
Solution: This hotfix updates the OfficeScan program to ensure that the OfficeScan server can apply multiple policies from a Control Manager 6.0 server.

Hotfix_5015
Issue: The OfficeScan client computer may stop responding during a RealTime Scan when both the Ravage Scan feature and the Browser Exploit Prevention feature are enabled.
Solution: This hotfix updates the OfficeScan agent program to ensure that it can run RealTime Scans normally when both the Ravage Scan feature and the Browser Exploit Prevention feature are enabled.

Hotfix_5016
Issue: Guest users that do not have the required permissions may be able to change certain OfficeScan 11.0 Service Pack 1 web console settings.
Solution: This hotfix adds RBA rules in "TrendAuthDef.xml" and enables the CGI console common to get more information from the XML file. This helps ensure that users that do not have the required permissions cannot make changes to the OfficeScan 11.0 Service Pack web console.

Hotfix_5018
Issue: An OfficeScan server without an Integrated Smart Protection Server (ISPS) installed can have a standalone Smart Protection Server (SPS) as the Smart Scan source. However, the "Standard Smart Protection Server List" page of the web console indicates that the Smart Scan source is ISPS when OfficeScan is using an SPS. The issue occurs after users install Critical Patch 4150 on the OfficeScan server.
Solution: This hotfix ensures that the correct Smart Scan source appears on the "Standard Smart Protection Server List" page.

Hotfix_5020
Issue 1: When users right-click the OfficeScan agent icon on the system tray and select "Advanced Schedule Scan Setting" to access the "Scheduled Scan Postpone" dialog box, they can only set the postpone hour time interval up to "11" hours even
when the field should support up to "12" hours.

**Solution 1:** This hotfix updates the OfficeScan agent program to allow users to set the Scheduled Scan Postpone hour time interval to "12" hours.

**Issue 2:** 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 2:** 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.

**Hotfix_5020.1**

**Issue 1:** When users right-click the OfficeScan agent icon on the system tray and select "Advanced Schedule Scan Setting" to access the "Scheduled Scan Postpone" dialog box, they can only set the postpone hour time interval up to "11" hours even when the field should support up to "12" hours.

**Solution 1:** This hotfix updates the OfficeScan agent program to allow users to set the Scheduled Scan Postpone hour time interval to "12" hours.

**Issue 2:** 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 2:** 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.

**Hotfix_5024**

**Issue:** Users encounter an error while decoding virus files using the VSEncode tool.

**Solution:** This hotfix updates the OfficeScan server program files to ensure that VSEncode can decode virus files without issues.

**Hotfix_5028**

**Issue:** When users install an OfficeScan agent on a computer running on the 32-bit version of Microsoft(TM) Windows(TM) 10 Anniversary Update 1607.14393 using a setup package created by the Agent Packager tool, the OfficeScan agent will still be installed on the default installation path even when a new path has been specified.

**Solution:** This hotfix resolves the issue by updating the OfficeScan server program to ensure that setup packages created by the Agent Packager tool installs OfficeScan agents on the specified installation paths.

**Hotfix_5029**
**Issue:** Users encounter a high CPU usage issues when OfficeScan browser plugins are enabled on the version 11 of the Internet Explorer web browser.

**Solution:** This hotfix updates the BEP module to prevent the high CPU usage issue.

**Hotfix_5030**

**Issue:** When users export the Scan Exclusion Lists for the following scan types from the "Agent Management" screen of the OfficeScan web console, the generated CSV file will not contain any domain setting information for OfficeScan agents:
- Manual scans
- Real-time scans
- Scheduled scans
- Scan Now

**Solution:** This hotfix updates the OfficeScan server files to ensure that when users export Scan Exclusion Lists, the domain setting information for each OfficeScan agent appear on the exported CSV files.

**Hotfix_5031**

**Issue:** Users encounter a high CPU usage issues when OfficeScan browser plugins are enabled on the version 11 of the Internet Explorer web browser.

**Solution:** This hotfix updates the BEP module to prevent the high CPU usage issue.

**Hotfix_5032**

**Issue:** The "Resume an interrupted Scheduled Scan" option in the Scheduled Scan Settings does not work if a scheduled scan was interrupted because the endpoint was switched off.

**Solution:** This hotfix updates the OfficeScan agent program to ensure that the "Resume an interrupted Scheduled Scan" feature works properly.

**Hotfix_5033**

**Issue:** The OfficeScan web console cannot display the firewall exception list properly if the number of exceptions in a firewall policy is a multiple of 249.

**Solution:** This hotfix updates the OfficeScan server programs to ensure that the OfficeScan web console can successfully display the firewall exception list when the number of exceptions in a firewall policy is a multiple of 249.

**Hotfix_5037**

**Issue:** The "Real-time Scan Health Check" feature in OfficeScan agent regularly sends its status to the server even when this feature is disabled. This adds to the network traffic.
**Solution:** This hotfix updates the OfficeScan agent program to ensure that it does not send "Real-time Scan Health Check" network packets to the server when the feature is disabled.

**Hotfix_5038**

**Issue 1:** The OfficeScan NT Listener service stops responding while managing the Suspicious Connection Service NCIE function on OfficeScan agents.

**Solution 1:** This hotfix updates the OfficeScan agent program to improve the way the TmListen service manages the NCIE function.

**Issue 2:** A memory allocation issue related to the "OfcNotifyQueue.dll" file can lead to memory leaks which may trigger "OfcServer.exe" to stop unexpectedly.

**Solution 2:** This hotfix resolves the memory allocation issue to prevent memory leaks.

**Hotfix_5070**

**Issue:** The Ransomware Protection function does not reference the prevalence value and simply terminates the processes (even if these processes meet the expected prevalence value)

**Solution:** This hotfix ensures that OfficeScan agents check the process chain for Ransomware identification in this situation. The OfficeScan agents will query the census server for all parent processes and determine whether or not to terminate the process.

Below are the issues resolved by the hot fixes in OSCE 11.0 SP1 CP4150:

**Hotfix_6067**

**Issue:** In some situation, the Meerkat function in 32 bit platform might not work correctly in previous AEGIS build.

**Solution:** This hotfix provide the new build of AEGIS module to fix above of issue.

**Hotfix_6080**

**Issue:** An issue related to the "tmeectv.dll" module in OfficeScan 11.0 Service Pack 1 with Critical Patch 6054 may trigger a handle leak issue.

**Solution:** This hot fix updates the OfficeScan 11.0 Service Pack 1 with Critical Patch 6054 agent files to prevent the handle leak issue.

**Hotfix_6082**

**Issue:** A handle leak issue that may occur while the OfficeScan server handles the "ofcserv

**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.

Hotfix_6084
Issue: Users are unable to subscribe to the Control Manager server to get the suspicious object list. They receive a "-1" return error.
Solution: This hot fix resolves the subscription issue by installing and enabling Local Web Classification Server (LWCS), instead of LWCS being enabled only.

Hotfix_6084.1
Issue: The User Mode Hooking (UMH) driver causes an unexpected error.
Solution: This hot fix updates the UMH driver to resolve the issue.

Hotfix_6084.2
Issue 1: OfficeScan continues to scan network drives even if the "Scan network drive" setting is disabled in Real-time Scan.
Solution 1: This hotfix ensures that OfficeScan correctly implements the "Scan network drive" setting when performing Real-time Scan.
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.

Hotfix_6085
Issue: Data Loss Prevention Endpoint causes a Blue Screen of Death (BSoD) on Microsoft(TM) Windows(TM) 10 Redstone.
Solution: This hot fix resolves the BSoD issue on Windows 10 Redstone.

Hotfix_6085.1
Issue: Users are unable to save the settings in the "Device Control Settings" page of the OfficeScan web console. This situation occurs if they edit the page by selecting the root domain icon in the "Agent Management" page of the OfficeScan web console.
Solution: This hot fix updates the OfficeScan server program to resolve this issue.

Hotfix_6088
Issue: When using the Microsoft(TM) Windows domain user account to migrate an OfficeScan database from codebase to an SQL database, a "conhost.exe" application error might occur while updating the SQL schema.
**Solution:** This hotfix uses another method when handling the SQL schema update instead of using the Windows application program interface (API), which resolves this issue.

Hotfix_6091

**Issue:** The OfficeScan Update Agent does not deploy the Suspicious Connection Settings to OfficeScan clients.

**Solution:** This hotfix ensures that the OfficeScan Update Agent deploys the Suspicious Connection Settings to OfficeScan clients.

Hotfix_6094

**Issue:** Users encounter an issue wherein they are unable to open Microsoft(TM) Office 2007 documents from Microsoft SharePoint 2010 after installing Critical Patch (CP) 6054.

**Solution:** This hotfix improves on the DRE module of OfficeScan. Since DRE module does not back up the remote drive file, AEGIS (Behavior Monitoring) should skip sending remote drive file events to the DRE module.

Hotfix_6098

**Issue:** 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 server and agent files to allow users to assign agents to pre-defined multilayer domains.

Hotfix_6101

**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.

Hotfix_6103

**Issue:** The "Global Agent Settings" page of the OfficeScan 11.0 Service Pack 1 German version console contains mistranslated information.

**Solution:** This hotfix ensures that all the information on the page are translated correctly.

Hotfix_6106

**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.

**Hotfix_6110**  
**Issue**: The listDeviceInfo tool cannot display any information about a special USB device if its device information is not in the usual format.  
**Solution**: This hotfix updates the "listDeviceInfo.exe" tool to enable it to display information about USB devices when the device information is not in the usual format.

**Hotfix_6111**  
**Issue**: A memory allocation issue related to the "OfcNotifyQueue.dll" file can lead to memory leaks which may trigger "OfcServer.exe" to stop unexpectedly.  
**Solution**: This hotfix resolves the memory allocation issue to prevent memory leaks.

**Hotfix_6111.1**  
**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".

**Hotfix_6112**  
**Issue 1**: When the Behavior Monitoring service stops unexpectedly, it automatically notifies all its plug-ins to stop. However, an issue may prevent it from notifying the User Mode Event Hooking plug-in which results in a high CPU usage issue.  
**Solution 1**: This hotfix ensures that OfficeScan notifies the User Mode Event Hooking plug-in to stop sending events while the Behavior Monitoring service detects an unhandled exception and to de-initialize itself. This helps prevent the high CPU issue when the Behavior Monitoring service stops unexpectedly.  
**Issue 2**: Some privilege issues occur when DRE attempts to access a file on a UNC path that breaks the existing UNC path connection.  
**Solution 2**: This hotfix ensures that the OfficeScan DRE feature works normally on UNC paths.

**Hotfix_6114**  
**Issue**: An issue prevents users from accessing the "DLP Settings" and "Device control
Settings" pages of the OfficeScan server console.

**Solution**: This hotfix updates the server program to ensure that users can access the pages normally.

**Hotfix_6118**

**Issue 1**: When users attempt to print documents through a Microsoft(TM) Windows(TM) 32-bit application in an x64 platform, the corresponding Trend Micro Data Loss Prevention(TM) (DLP) violation log refers to a CD/DVD channel.

**Solution 1**: This hotfix ensures that the corresponding DLP violation logs refers to the correct channel.

**Issue 2**: Users can run an application under USB storage devices that they only have READ permission to access.

**Solution 2**: This hotfix ensures that only users with the correct application permission can run applications under USB storage devices.

**Hotfix_6120**

**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**: When using the "Sort Agent" option to group OfficeScan agents based on the Active Directory structure, an unexpected domain structure is created on the Agent Management screen.

**Solution 2**: This hotfix updates the OfficeScan server to display the correct Active Directory domain structure on the Agent Management screen after sorting agents based on Active Directory.

**Hotfix_6121**

**Issue**: If an OfficeScan agent encounters a connection issue while it is being moved from one OfficeScan server to another, the OfficeScan agent does not unregister from the original server.

**Solution**: This hotfix ensures that the OfficeScan agent properly unregisters from its original OfficeScan server if a connection issue occurs.

**Hotfix_6122**

**Issue**: The OfficeScan 11.0 Service Pack 1 Behavior Monitoring feature blocks a valid program.

**Solution**: This hotfix updates the OfficeScan Behavior Monitoring Local Pattern to ensure that it blocks the correct programs.
Hotfix_6126

**Issue**: When the OfficeScan agent scans for virus and malware in a compressed file, the corresponding Scan Operation Logs display inaccurate total number of detected virus and malware.

**Solution**: This hotfix updates the OfficeScan agent files to ensure that the Scan Operation Logs display the correct total number of virus and malware detected from compressed files.

Hotfix_6126.1

**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.

Hotfix_6127

**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.

Hotfix_6130

**Issue**: The OfficeScan 11.0 Service Pack 1 Behavior Monitoring feature blocks a valid program.

**Solution**: This hotfix updates the OfficeScan Behavior Monitoring Local Pattern to ensure that it blocks the correct programs.

Hotfix_6131

**Issue**: The OfficeScan 11.0 Service Pack 1 server program and the OfficeScan agent Smart Scan common module uses an OpenSSL version that is affected by certain vulnerabilities.

**Solution**: This hotfix resolves this issue by updating the OpenSSL component of the server module and Smart Scan common module.

Hotfix_6133

**Issue**: When the OfficeScan server manages database queries, sometimes the query process creates a large number of Que*.tmp files in the "HTTPDB" folder and these
files are not removed promptly after the query process completes.

**Solution:** This hotfix updates the OfficeScan server files to enhance the error management mechanism for database query processing to limit the number of Que*.tmp files and ensure that these files are deleted promptly after a query has been processed completely.

**Hotfix_6135**

**Issue:** BSOD occurs when the firewall rule has too many filters.

**Solution:** This hotfix updates the Network Security Components to prevent the BSOD issue.

**Hotfix_6135.1**

**Issue:** BSOD occurs when the firewall rule has too many filters.

**Solution:** This hotfix updates the Network Security Components to prevent the BSOD issue.

**Hotfix_6136**

**Issue 1:** OfficeScan Data Loss Prevention (DLP) is unable to block the CD/DVD burning function of explorer.exe in "USB flash drive" mode.

**Solution 1:** The hot fix resolves the DLP blocking issue.

**Issue 2:** Data Loss Prevention only generates a maximum of 200 violation logs even if users burn more than 200 files (with violations) using the CD/DVD player function of explorer.exe.

**Solution 2:** The hot fix resolves the issue by enlarging the queue size to 100,000.

**Hotfix_6138**

**Issue:** When users assess for unmanaged endpoints, the results for computers that appear "Online" on the product tree is "Unresolved Active Directory Assessment". This occurs because the AD_GUID vectors queried from the Active Directory (AD) domain server are uppercase or lowercase variants of vectors queried from the database.

**Solution:** This hotfix makes the comparison mechanism case-insensitive to ensure that users can accurately assess endpoints.

**Hotfix_6140**

**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.
Hotfix_6140.1

**Issue**: After an OfficeScan agent is remotely installed on a computer, the OfficeScan server maps a new network driver for the installation. Sometimes, these network drivers are not removed and remain on the server.

**Solution**: This hotfix updates the agent remote installation process to ensure that it removes the mapped network drivers automatically after agent installation.

Hotfix_6141

**Issue 1**: An issue prevents the DLP module from blocking attachments that contain sensitive information in Outlook Web App 2003 and 2010.

**Solution 1**: This hotfix ensures that the DLP module can block attachments with sensitive information in Outlook Web App 2003 and 2010.

**Issue 2**: An issue related to the scanning of traffic to and from SCOM results in a high disk space usage issue in the "dgtmpmon" folder.

**Solution 2**: This hotfix prevents the high disk space usage issue.

Hotfix_6147

**Issue**: When users run the Agent Packager tool in the CLI to create setup or update packages for the OfficeScan agent, there is no way to specify a domain where all freshly-installed clients should belong to.

**Solution**: This hotfix updates the Agent Packager tool to enable users to specify a domain for freshly-installed agents using the "/domain" parameter when creating setup or update packages for the OfficeScan agent through the CLI.

Hotfix_6148

**Issue**: OfficeScan security compliance reports indicate that the WRS is non-compliant because OfficeScan treats the database service switch flag as the WRS flag.

**Solution**: This hotfix updates the server program to ensure that it reads the WRS flag from the "ofcscan.ini" file.

Hotfix_6149

**Issue**: The ransomware count on the Ransomware Widget does not include all ransomware file detections because the new ransomware detection log label starts with "Ransom."

**Solution**: This hotfix enables the Ransomware Widget to include ransomware detection logs that start with "Ransom." in the ransomware count.

Hotfix_6151

**Issue**: The following services provide robust protection but their monitoring
mechanisms can strain system resources, especially on Windows server platforms:
- Unauthorized Change Prevention Service
- Suspicious Connection Service
- Advanced Protection Service
For this reason, these services are disabled by default on Windows Server 2003, 2008, and 2012.

**Solution:** This hotfix allows users to enable the services above by default on a freshly installed OfficeScan agent on the Windows Server platform.

**Hotfix_6152**

**Issue:** The DLP module of the OfficeScan agent program may not be able to upgrade successfully if its registry entry is corrupted.

**Solution:** This hotfix updates the OfficeScan agent program to ensure that the DLP module can update successfully.

**Hotfix_6155**

**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.

**Hotfix_6157**

**Issue:** An incompatibility issue between the OfficeScan Advanced Protection Service and the OfficeScan Unauthorized Change Prevention Service may cause the OfficeScan Common Client **Solution** Framework (TMCCSF.exe) service to stop unexpectedly.

**Solution:** This hotfix resolves the issue by updating the OfficeScan Common Client **Solution** Framework module in OfficeScan 11.0 Service Pack 1.

**Hotfix_6158**

**Issue:** The TmCCSF.exe process may trigger a high CPU usage issue when the Advanced Protection Service is enabled.

**Solution:** This hotfix updates OfficeScan agent program to prevent the high CPU usage issue.

**Hotfix_6167**

**Issue:** On OfficeScan agents, the "Ntrtscan.exe" process stops repeatedly because it cannot start the VSAPI driver.

**Solution:** This hotfix updates the OfficeScan agent program to ensure that
"Ntrtscan.exe" starts and works normally.

Hotfix_6170

**Issue:** A mismatch issue between the encode and decode calling mechanism prevents the OfficeScan server from syncing up with the AD domain.

**Solution:** This hotfix resolves the issue by updating the OfficeScan server program to ensure that the OfficeScan server syncs up with the AD domain properly.

Hotfix_6178

**Issue 1:** Several abnormal messages appear on the Windows 10 Red Stone platform even when the ping results are successful.

**Solution 1:** This hotfix updates the OfficeScan agent program to prevent the abnormal messages in computers running on the Windows 10 Red Stone platform.

**Issue 2:** The OfficeScan agent may not be able to scan a file successfully if the file is specified by a UNC path.

**Solution 2:** This hotfix updates an agent file to ensure that the OfficeScan agent can scan files specified using UNC paths successfully.

Hotfix_6182

**Issue:** When an OfficeScan 11.0 Service Pack 1 agent is configured not to upload firewall logs, it may automatically start uploading these logs after restarting.

**Solution:** This hotfix updates the OfficeScan agent program to ensure that OfficeScan agents upload firewall logs only when enabled to do so.

Hotfix_6184

**Issue:** The OfficeScan web console cannot display the firewall exception list properly if the number of exceptions in a firewall policy is a multiple of 249.

**Solution:** This hotfix updates the OfficeScan server programs to ensure that the OfficeScan web console can successfully display the firewall exception list when the number of exceptions in a firewall policy is a multiple of 249.

Hotfix_6185

**Issue:** If the OfficeScan agent does not have Windows Update enabled or is located in an isolated network environment, it may not be able to update its pattern files from the OfficeScan server, even when an active connection is available. This happens because the signature check failed of ActiveUpdate module and the OfficeScan agent is unable to complete downloading and merging pattern files.

**Solution:** This hotfix updates the ActiveUpdate module to ensure that the OfficeScan agent can successfully update its pattern files from the OfficeScan server.
Hotfix_6187

**Issue**: OfficeScan Data Protection causes Google(TM) Chrome version 53.0.2785.116 hang.

**Solution**: This hotfix resolves the hang issue when Chrome is running on its QUIC mode.

Hotfix_6190

**Issue**: USB Floppy cannot be added into Exception of Removable Storage of OfficeScan Data Protection(DLP) Policy Settings.

**Solution**: This hotfix resolves can add USB Floppy into Exception of Removable Storage of DLP Policy Settings.

Hotfix_6193

**Issue 1**: Several abnormal messages appear on the Windows 10 Red Stone platform even when the ping results are successful.

**Solution 1**: This hotfix updates the OfficeScan agent program to prevent the abnormal messages in computers running on the Windows 10 Red Stone platform.

**Issue 2**: The OfficeScan agent may not be able to scan a file successfully if the file is specified by a UNC path.

**Solution 2**: This hotfix updates an agent file to ensure that the OfficeScan agent can scan files specified using UNC paths successfully.

Hotfix_6196

**Issue 1**: Some drivers cannot be loaded in Microsoft(TM) Windows(TM) 10 when both UEFI and Secure Boot are enabled.

**Solution 1**: This hotfix updates a new driver with the "Microsoft Windows Hardware Compatibility Publisher" digital signature to ensure that drivers can be loaded successfully.

**Issue 2**: The Avaya Scopia(TM) log in page stops responding when the AEGIS module does not receive a response from it within a specific time period.

**Solution 2**: This hotfix enables users to disable the self-protection feature of the AEGIS module for Avaya Scopia to prevent the incompatibility issue and ensure that Avaya Scopia runs normally on protected computers.

**Issue 3**: After upgrading to OfficeScan 11.0 Service Pack 1 Build 6134, the OfficeScan web console stops responding when users delete a domain in the "Agent Management > Manage Agent Tree > Remove Domain/Agent" screen.

**Solution 3**: This hotfix ensures that users can delete domains normally in the "Agent Management > Manage Agent Tree > Remove Domain/Agent" screen.
Hotfix_6209

**Issue:** Sometimes, the wrong license information appears on the OfficeScan "Product License" page after users click on the "Update Information" button.

**Solution:** This hotfix ensures that the "Update Information" button works normally and that the correct license information appears on the OfficeScan "Product License" page.

Hotfix_6212

**Issue 1:** The UMH driver triggers an unexpected error.

**Solution 1:** This hotfix updates the UMH driver to resolve the issue.

**Issue 2:** The UMH driver triggers an unexpected error in the Windows 10 Red Stone platform.

**Solution 2:** This hotfix updates the UMH driver to resolve the issue.

Hotfix_6213

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

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

Hotfix_6213.1

**Issue:** When users deploy an OfficeScan policy from Control Manager using the "PolicyExportTool.exe" utility, the exported policy displays the wrong component type for the comOSCECCCA component.

**Solution:** This hotfix ensures that when the "PolicyExportTool.exe" utility exports OfficeScan policies from Control Manager, the exported policies display the correct component types.

Hotfix_6214

**Issue:** The "Date/Time" field on the "Spyware/Grayware Log" page of the OfficeScan server console displays the time when the server received each Security Risk log instead of the date and time that a malware was detected on an OfficeScan agent.

**Solution:** This hotfix corrects the "Date/Time" information on the "Spyware/Grayware Log" page.

Hotfix_6216
**Issue:** The Avaya Scopia log in page stops responding when the AEGIS module does not receive a response from it within a specific time period.

**Solution:** This hotfix enables users to disable the self-protection feature of the AEGIS module for Avaya Scopia to prevent the incompatibility issue and ensure that Avaya Scopia can run normally on protected computers.

**Enhancements**

Below are the enhancements of the hot fixes in OSCE 11.0:

**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:
  - BKAV Endpoint 11 version 3690
  - ESET Endpoint Antivirus 5.0.2229.1
  - Kaspersky Endpoint Security 10 for Windows 10.2.1.23
  - Kaspersky Endpoint Security 10 for Windows 10.2.2.10535
  - Kaspersky Endpoint Security 8 for Windows 8.1.0.646
  - Kaspersky Endpoint Security Center Network Agent 10.1.249
  - McAfee Agent 4.5.0.1499
  - McAfee Agent 4.5.0.1810
  - McAfee Agent 4.5.0.1852
  - McAfee Agent 4.8.0.887 (x86/x64)
  - McAfee VirusScan Enterprise 8.7.00003
  - McAfee VirusScan Enterprise 8.8.0.1247 (x86/x64)
  - Sophos Anti-Virus 10.0.5
  - Sophos Anti-Virus 10.3.7 (x86/x64)
  - Sophos Anti-Virus NT 10.3.13
  - Sophos Auto Update 3.1.1.8 (x86/x64)
- Sophos Auto Update 4.1.0.273 (x86/x64)
- Sophos Client Firewall 2.9.0
- Sophos Patch Agent 1.0.303.0 (x86/x64)
- Sophos Remote Management System 3.2.0 (x64)
- Sophos Remote Management System 3.4.0
- Sophos Remote Management System 3.4.1 (x64)
- Sophos Technical Support 10.0.5 (X64)
- Symantec AntiVirus 12.1.5337.5000 x32
- Symantec AntiVirus 12.1.5337.5000 x64
- Symantec Endpoint Protection 12.1.2015.2015 (x86/x64)
- Symantec Endpoint Protection 12.1.6168.6000 (x86/x64)
- Symantec Endpoint Protection 12.1.617.4971 (x86/x64)
- Symantec(TM) Endpoint Protection 12.1.3001.165

- The Japanese versions of the following third-party products with the Japanese version of OfficeScan:
  - ePOAgent1000
  - ePOAgent2000
  - ePOAgent3000
  - FFR yarai
  - Microsoft Forefront Client Security Antimalware Service : 1.5.1937.14
  - Microsoft Forefront Client Security Assessment Service : 1.0.1703.0
  - Symantec Endpoint Protection 12.1.1000.157 (x86)
  - Symantec Endpoint Protection 12.1.4013.4013 (x86/x64)
  - Symantec Endpoint Protection 12.1.4100.4126
  - Symantec Endpoint Protection 12.1.4100.4126
  - Symantec Endpoint Protection 12.1.4100.4126 (x64)
  - Symantec Endpoint Protection 12.1.4100.4126 (x86)

- The English versions of the following third-party products with the French version of OfficeScan:
  - Symantec(TM) Endpoint Protection 12.1.1000.157

**Hotfix_1783**

**Enhancement:** This hot fix enables Data Loss Prevention Endpoint SDK 6.0 to support up to version 40.0.2214.94 (32-bit) and 40.0.2214.94 (64-bit) of the Google Chrome web browser.

**Hotfix_1789.1**
Enhancement: This hot fix changes the command for generating certificates through the SvrSvcSetup.exe tool to "svrsvcsetup.exe -GenIISCert".

Hotfix_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.

Hotfix_1836

Hotfix_1844
Enhancement: This hot fix enables the Trend Micro Data Loss Prevention(TM) module in OfficeScan 11.0 to support the following:
- version 40.0a1 (2015-04-19) of the BETA release 64-bit Mozilla(TM) Firefox(TM) web browser
- up to version 42.0.2311.90 of the 32 and 64-bit Google Chrome(TM) web browser

Hotfix_1845
Enhancement: This hot fix updates the OfficeScan agent program and Virus Scan Engines to enhance the Files Self Protection function in OfficeScan agents.

Hotfix_1847
Enhancement: Support Diners Club credit card number in the "CreditCardNumber" validator.

Hotfix_1853
Enhancement: American Name validator is not case sensitive.

Hotfix_1874
Enhancement: This hot fix enables Data Loss Prevention Endpoint SDK 6.0 to support up to version 43.0.2357.81 of the 32 and 64-bit Google Chrome(TM) web browser.

Hotfix_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.

Hotfix_1914
**Enhancement:** This hot fix allows users to hide the "Unlock" button on the OfficeScan client console.

Hotfix_1915
**Enhancement:** This hot fix enables Data Loss Prevention Endpoint SDK 6.0 to support version 43 of the Firefox web browser.

Hotfix_1921
**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.

Hotfix_1924
**Enhancement:** This hot fix enables Data Loss Prevention Endpoint SDK 6.0 to support up to BETA version 44.0.2403.52 of the 32 and 64-bit Chrome web browser.

Hotfix_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.

Hotfix_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.

Hotfix_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.
**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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.

**Hotfix_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

Below are the enhancements of the hot fixes in OSCE 11.0 SP1:

**Enhancement:** Third-party Product Uninstallation - The OfficeScan installation program now automatically removes the following products before installing the OfficeScan client:

Hotfix_3011.u, Hotfix_3066.u, Hotfix_3610.u

- The English versions of the following third-party products with the English version
of OfficeScan:
- ESET Remote Administrator Agent 6.1.365.0 x86/x64
- ESET Remote Administrator Agent 6.1.444.0 x86/x64
- Kaspersky Endpoint Security 10 for Windows version 10.2.2.10535
- 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

Hotfix_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.

Hotfix_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.

Hotfix_3046
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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_3611
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.

Hotfix_3621
Enhancement: This hot fix enables users to create a list of approved URLs for the Osprey module and to deploy the list globally.

Hotfix_3645
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.

Hotfix_3655
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.

Hotfix_3679
Enhancement: This hot fix enables Data Loss Prevention(TM)(DLP) 6.0 to support Google(TM) Chrome version 49.0.2623.87.

Hotfix_3683
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.

Hotfix_3690
Enhancement: This hotfix enables the OfficeScan DLP module to show the file size information in violation logs.

Hotfix_3697
Enhancement: This hotfix enables OfficeScan to send the login password to connect to the Control Manager server by "POST" method.

Hotfix_3704
Enhancement: This hotfix enables the OfficeScan server to receive only the policies that have been updated instead of receiving all the policies each time the Control Manager 6.0 server deploys policies. This helps reduce the impact on OfficeScan's performance especially when the Control Manager 6.0 server runs regular policy enforcement.

Below are the enhancements of the hot fixes in OSCE 11.0 SP1 CP4150:

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:
  - AVG 2013 x64
  - AVG 2016 x64
  - F-Secure Client Security Premium 11.61 build 104 x86/x64
  - Kaspersky Endpoint Security 10 for Windows 10.2.4.674
  - McAfee Agent 4.8
  - McAfee Agent 4.8.0.1500
  - McAfee Agent 4.8.0.1938 x86/x64
  - McAfee Agent 5.0.2.188
  - Symantec Endpoint Protection 11.0.6005.562 x86/x64
  - Symantec Endpoint Protection 12.1.1101.401 x86/x64
  - Symantec Endpoint Protection 12.1.2015.2015 x86/x64
  - Symantec Endpoint Protection 12.1.4100.4126 x86/x64
  - Symantec Endpoint Protection 12.1.4112.4156 x86/x64
  - Symantec Endpoint Protection 12.1.671.4971 x86
  - McAfee ePOAgent3000
  - Panda Endpoint Agent 7.20.00.0000 x86
  - Panda Endpoint Protection 7.82.00.0000 x86
  - Sophos Anti-Virus 10.3.1 x86/x64
  - Sophos Anti-Virus 10.3.15 x86/x64
  - Sophos Anti-virus 10.3.15.69
  - Sophos Anti-Virus 10.6.3.537 x86/x64
  - Sophos Anti-Virus NT 10.2.6 x86/x64
  - Sophos AutoUpdate 2.9.0.344 x86/x64
  - Sophos AutoUpdate 4.3.10.27 x86/x64
  - Sophos AutoUpdate 5.2.0.276 x86/x64
  - Sophos Network Threat Protection 1.2.2.50 x86/x64
  - Sophos Remote Management System 3.4.1 x86/x64
  - Sophos Remote Management System 4.0.6 x86/x64
  - Sophos System Protection 1.3.0 x86/x64
  - Symantec Endpoint Protection 12.1.4013.4013 x86/x64
  - Symantec Endpoint Protection 12.1.5337.5000 x64/x86
  - Symantec Endpoint Protection 12.1.5337.5000 x86/x64
- Symantec Endpoint Protection 12.1.6608.6300 x86/x64
- Symantec Endpoint Protection 12.1.6318.6100 x64/x86
- Symantec Endpoint Protection 12.1.6318.6100 x86/x64
- Symantec Endpoint Protection 12.1.6860.6400 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 12.1.5337.5000 JP

- The Traditional Chinese versions of the following third-party products with the Traditional Chinese version of OfficeScan:
  - Kaspersky Endpoint Security 10.2.1.23 x86/x64
  - Kaspersky Network Agent 10.1.249 x86/x64

Hotfix_4168

Hotfix_4172
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.

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

Hotfix_4192
Enhancement: This hot fix allows users to hide the "Unlock" button on the
OfficeScan client console.

Hotfix_4201
Enhancement: This hot fix enables Data Loss Prevention Endpoint support generic url-encoded form post.

Hotfix_4207
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.

Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_4231
Enhancement: This hot fix enables users to create a list of approved URLs for the Osprey module and to deploy the list globally.

Hotfix_4249
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.

Hotfix_4262
Enhancement 1: This hot fix enables OfficeScan DLP module to support Google(TM) Chrome Beta version 48.0.2564.48.
**Enhancement 2:** This hot fix enables the OfficeScan DLP module to support dual signatures, SHA-1 and SHA-256.

**Hotfix_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)

**Hotfix_4273**  
**Enhancement:** This hot fix adds Trend Micro Behavior Monitor, hooking Microsoft Windows X86 ZwMapViewOfSection for ransomware detection.

**Hotfix_4281**  
**Enhancement:** This hot fix prevents the sequence "000000000000" from triggering the "Japan-My Number Individual" identifier.

**Hotfix_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.

**Hotfix_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.

**Hotfix_4300**  
**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.

**Hotfix_4306**  
**Enhancement:** This hot fix allows 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.

**Hotfix_4712**
**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.

Hotfix_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.

Hotfix_4733.1

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

Hotfix_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.

Hotfix_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.

Hotfix_4786

**Enhancement:** This hot fix prevents the sequence "000000000000" from triggering the "Japan-My Number Individual" identifier.

Hotfix_4833

**Enhancement:** This hot fix enables Data Loss Prevention(TM)(DLP) 6.0 to support Google(TM) Chrome version 49.0.2623.87.
Hotfix_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.

Hotfix_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.

Hotfix_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.

Hotfix_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

Hotfix_4901
**Enhancement:** This hot fix enables Data Loss Prevention(TM)(DLP) 6.0 to support Google(TM) Chrome version 50.0.2661.94.

Hotfix_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.

Hotfix_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.

Hotfix_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.
Hotfix_4934
**Enhancement:** This hotfix enables users to configure the OfficeScan server to notify OfficeScan agents to stop communicating with the census server while restarting.

Hotfix_4939
**Enhancement:** This hotfix enhances the performance of the OfficeScan DLP URL retrieving function to ensure that it runs normally while users drag and drop files to upload these files in Google Chrome.

Hotfix_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.

Hotfix_4948
**Enhancement:** This hotfix enhances the performance of the OfficeScan DLP URL retrieving function to ensure that it runs normally while users drag and drop files to upload these files in Google Chrome.

Hotfix_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.

Hotfix_4965.1
**Enhancement 1:** DLP enhances the ability of the HTTP Parser for IBM Domino Web Access, allowing it to record more detailed information in violation events.  
**Enhancement 2:** DLP implements a Webmail exception for Domino Web Access.

Hotfix_4978
**Enhancement:** This hot fix enables OfficeScan Data Loss Prevention (DLP) to increase the limit of the DLP archive file setting on the web console.

Hotfix_4983
**Enhancement:** This hot fix provides an option to enable the permission feature on an OfficeScan server and to automatically deploy the setting to OfficeScan agents.
Hotfix_4983.1

**Enhancement:** This hotfix enables the OfficeScan agent installation program to check for third-party antivirus products before installing the OfficeScan agent program on a computer. After applying this hotfix, users will be able to configure the agent installation program to automatically uninstall specific third-party antivirus products before installation.

Hotfix_5007.1

**Enhancement:** This hotfix provides a way for users to configure Trend Micro Data Loss Prevention(TM) (DLP) Endpoint SDK 6.0 to load the converter dynamic library instead of using "dtoop.exe".

Hotfix_5009

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

Hotfix_5009.1

**Enhancement:** This hotfix enables the OfficeScan agent installation program to check for third-party antivirus products before installing the OfficeScan agent program on a computer. After applying this hotfix, users will be able to configure the agent installation program to automatically uninstall specific third-party antivirus products before installation.

Hotfix_5014

**Enhancement:** This hotfix enables the OfficeScan server to receive only the policies that have been updated instead of receiving all the policies each time the Control Manager 6.0 server deploys policies. This helps reduce the impact on OfficeScan's performance especially when the Control Manager 6.0 server runs regular policy enforcement.

Below are the enhancements of the hot fixes in OSCE 11.0 SP1 CP6054:

**Enhancement:** Third-party Product Uninstallation - The OfficeScan installation program now automatically removes the following products before installing the OfficeScan client:

- Hotfix_6087.u
- Hotfix_6090.u
- Hotfix_6097.u
- Hotfix_6104.u
- Hotfix_6108.u
- Hotfix_6132.u
- Hotfix_6142.u
- Hotfix_6152.u
- Hotfix_6153.u
- Hotfix_6165.u
- The English versions of the following third-party products with the English version of OfficeScan:
  - Avira Server Security 13.0.0.3736 x86/x64
  - ESET NOD32 Antivirus 3.0.669.0 x86/64
  - ESET NOD32 Antivirus 4.2.40.27 CHT x86/64
  - ESET NOD32 Antivirus 9.0.377.1 x86/64
  - Kaspersky 10.0.3361
  - Panda Free Antivirus 7.84.00.0000 x86/x64
  - Panda Free Antivirus 8.20.00.0000 x86/x64
  - Sophos 10.3
  - Sophos 10.5
  - Sophos 10.6
  - Sophos Anti-Virus 10.6.3.537 x86/x64
  - Sophos AutoUpdate 5.2.0.276 x86/x64
  - Sophos Client Firewall 2.9.5 x86/x64
  - Sophos Network Threat Protection 1.2.2.50 x86/x64
  - Sophos Patch Agent 1.0.308.0 x86/x64
  - Sophos Remote Management System 4.0.6 x86/x64
  - Sophos System Protection 1.3.0 x86/x64
  - Symantec Endpoint Protection 12.1.3001.165 x86/x64
  - Symantec Endpoint Protection 12.1.4100.4126 x86/x64
  - Symantec Endpoint Protection 12.1.5337.5000 x86/64
  - Symantec Endpoint Protection 12.1.6168.6000 x86/x64
  - Symantec Endpoint Protection 12.1.6860.6400 x86/x64
  - Symantec Endpoint Protection 12.1.6867.6400 x64
  - System Center Endpoint Protection 4.5.216.0 x86/x64

- The Japanese versions of the following third-party products with the Japanese version of OfficeScan:
  - McAfee Agent 4.8.0.641 x86/x64
  - McAfee VirusScan Enterprise 8.8.02004 x86/x64

- The French versions of the following third-party products with the French version of OfficeScan:
  - Symantec Endpoint Protection 12.1.4100.4126 x86 FR
**Enhancement**: This critical patch adds new core modules in OfficeScan 11.0 Service Pack 1 that enables it to work well with Windows 10 Red Stone 1 (Windows 10 Anniversary Update).

Hotfix_6077
**Enhancement**: This hotfix enables DLP Endpoint SDK 6.0 to support Chrome 51.0.2704.84m with QUIC enabled.

Hotfix_6088
**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.

Hotfix_6093
**Enhancement**: This hotfix enables DLP Endpoint SDK 6.0 to support Chrome 51.0.2704.106m with QUIC enabled.

Hotfix_6105
**Enhancement**: This hotfix enables users to add the "Offline Time" column to the Agent Management tree and to add the same information to CSV files exported through the "Agent Management" page of the OfficeScan web console. This column displays the time and date information of the last instance when the OfficeScan agent cannot connect to the OfficeScan server.  Note: After applying this hot fix, the order of columns in the Agent Management tree will be reset to the default order.

Hotfix_6109
**Enhancement**: This hotfix upgrades the Web Blocking Service module to support IP lookup when there are no results for URL lookup.

Hotfix_6120
**Enhancement**: This hotfix enables users to add the "Offline Time" column to the Agent Management tree and to add the same information to CSV files exported through the "Agent Management" page of the OfficeScan web console. This column displays the time and date information of the last instance when the OfficeScan agent cannot connect to the OfficeScan server.  Note: After applying this hot fix, the order of columns in the Agent Management tree will be reset to the default order.
Hotfix_6128
**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.

Hotfix_6129
**Enhancement 1**: This hotfix enables users to configure the OfficeScan server to check if the UID of an agent exists in the database by generating a compliance report and to notify the client machine to register again if it has no record of the agent's UID.

**Enhancement 2**: 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.

Hotfix_6167
**Enhancement 1**: This hotfix enables the OfficeScan agent installation program to check for third-party antivirus products before installing the OfficeScan agent program on a computer.

After applying this hotfix, users will be able to configure the agent installation program to automatically uninstall specific third-party antivirus products before installation.

**Enhancement 2**: This hot fix provides an option to enable the permission feature on an OfficeScan server and to automatically deploy the setting to OfficeScan agents.

Hotfix_6167.1
**Enhancement**: OfficeScan and Data Loss Prevention (DLP) starts support multiple forensic data session in the violation logs.

Hotfix_6168
**Enhancement**: This hot fix provides an option to enable the permission feature on an OfficeScan server and to automatically deploy the setting to OfficeScan agents.

Hotfix_6177
**Enhancement**: This hotfix provides a way for users to enable or disable the Osprey async mode.

Hotfix_6181
**Enhancement 1**: This hotfix enables users to configure the OfficeScan server to check if the UID of an agent exists in the database by generating a compliance report and to notify the client machine to register again if it has no record of the agent's UID.
**Enhancement 2**: 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.

**Hotfix_6183**

**Enhancement**: This hotfix improves the checking mechanism of the OfficeScan agent program to protect the Smart Scan Agent Pattern and Virus Pattern files in endpoints from corruption.

**Hotfix_6199**

**Enhancement**: This hotfix improves the index mechanism for the SQL table containing the OfficeScan agent information.