OfficeScan XG Patch 1 Merge List

Issues Resolved by Hot Fixes & Critical Patches

Table of Contents

Issues resolved by hot fixes for OfficeScan 10.6 Service Pack 3

Hot Fix B5921	Hot Fix B5921.1	Hot Fix B6010.1	Hot Fix B6011	Hot Fix B6014	Hot Fix B6016	Hot Fix B6019	Hot Fix B6020
Hot Fix B6028	Hot Fix B6030	Hot Fix B6031	Hot Fix B6033	Hot Fix B6036			

Hot Fix Build 5921 (SBM 332339)

Issue

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

Solution

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

Hot Fix Build 5921.1 (SBM 331874)

Issue

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

Solution

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

Hot Fix Build 6010.1 (SBM 347968)

Issue

Users may not be able to eject the USB device properly after scanning the files in the USB device.

Solution

This hot fix updates the OfficeScan client program that can correctly eject the USB device after scanning the files in the USB device.

Hot Fix Build 6011 (SBM 347807)

Issue

Data Loss Prevention™ Endpoint causes a Blue Screen of Death (BSoD) on Windows™ 10 Red Stone 1.

Solution

This hot fix resolves the BSoD issue on Windows™ 10 Red Stone 1.

Hot Fix Build 6014 (SBM 336883)

Enhancement

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

Hot Fix Build 6016 (SBM 46368)

Issue

BSOD occurs when the firewall rule has too many filters.

Solution

This hot fix updates the Network Security Components to prevent the BSOD issue.

NOTE 🗎 OfficeScan client computers should be restarted immediately after installing this hot fix to be able to use the newly-deployed NSC modules.

Hot Fix Build 6019 (SBM 349561)

Issue

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

Solution

This hot fix updates the OfficeScan client program to ensure that it uploads DLP violation logs to the OfficeScan server normally.

Procedure

To prevent the OfficeScan client from sending duplicate DLP violation logs to the OfficeScan server:

a. Install this hot fix (see Installation).

b. Open the Ofcscan.ini file in the \PCCSRV\ folder on the OfficeScan server installation directory.

c. Under the Global Setting section, manually add the ReindexDLPViolationLog key and set its value to "1".

[Global Setting]

ReindexDLPViolationLog = 1

NOTE To disable the feature, set "ReindexDLPViolationLog = 0".

d. Save the changes and close the file.

e. Open the OfficeScan web console and go to the **Networked Computers** > **Global Client Settings** screen.

f. Click **Save** to deploy the setting to clients.

The OfficeScan server deploys the command to OfficeScan clients and adds the following registry entry on all OfficeScan client computers:

Path: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

Key: ReindexDLPViolationLog

Type: dword

Value: 1

Hot Fix Build 6020 (SBM 350332)

Issue 1

OfficeScan Data Loss Prevention™ (DLP) is unable to 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.

Hot Fix Build 6028 (SBM 350974)

Issue

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.

Procedure

To enable the AU module to check certificates:

a. Install this hot fix (see Installation).

b. Open the aucfg.ini file in the \PCCSRV\web\service folder of the OfficeScan server.

c. Manually add the following key and set it to "1".

check_file_signature = 1

> NOTE To disable the certificate checking feature in the AU module, set "check_file_signature = 0".

d. Save the changes and close the file.

Hot Fix Build 6030 (SBM 350165)

Issue

Sometimes, the Behavior Monitoring Service module of OfficeScan 10.6 Service Pack 3 clients running on Windows 10 may disable the Wireless LAN when the client computer returns from Connected Standby Mode.

Solution

This hot fix updates the Behavior Monitoring Service module and the OfficeScan client program and allows users to set the period of time that OfficeScan has to wait before starting drivers when the

computer returns from Connected Standby Mode. This can help ensure that the Wireless LAN works normally after a client computer returns from Connected Standby Mode.

Procedure

To set the period of time in seconds that OfficeScan has to wait before starting drivers when the computer returns from Connected Standby Mode:

a. Install this hot fix (see Installation).

b. Open the Ofcscan.ini file in the \PCCSRV\ folder on the OfficeScan server installation directory.

c. Under the Global Setting section, manually add the PowerMonitorTime key and set the preferred value. Trend Micro recommends setting the value to "10".

   [Global Setting]

   PowerMonitorTime = 10

> NOTE This key supports any value between 1 and 60 seconds. To disable the feature, set "PowerMonitorTime = 0".

d. Save the changes and close the file.

e. Open the OfficeScan web console and go to the **Networked Computers** > **Global Client Settings** screen.

f. Click **Save** to deploy the setting to clients. The OfficeScan server deploys the command to OfficeScan clients and adds the following registry entry on all OfficeScan client computers:

   Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AEGIS

   Key: PowerMonitorTime

   Type: dword

   Value: 0, 1-60 seconds

g. Restart the OfficeScan clients.

Hot Fix Build 6031 (SBM 356934)

Issue

The OfficeScan 10.6 Service Pack 3 server program and the OfficeScan client Smart Scan common module uses an OpenSSL version that is affected by certain vulnerabilities.

Solution

This hot fix resolves this issue by updating the OpenSSL component of the server module and Smart Scan common module.

Hot Fix Build 6033 (SBM 356545)

Issue

The Microsoft™ Windows™ Defender sometimes still appears even if the OfficeScan client has been enabled.

Solution

This hot fix resolves this OfficeScan client issue by correctly changing the project settings.

Hot Fix Build 6036 (SBM 358232)

Enhancement

This hot fix enables users to configure OfficeScan clients to force unload a USB storage device if the number of viruses detected on the USB storage device exceeds a specified threshold.

Once unloaded, the USB storage device becomes invisible on the file explorer window which prevents users from accessing the USB storage device unless they plug in the device again.

Procedure

To enable the feature:

a. Install this hot fix (see Installation).
b. Open the ofcscan.ini file in the \PCCSRV\ folder on the OfficeScan installation directory.
c. Add the following key under the "Global Setting" section and set its value to "1".

   [Global Setting]

   UnloadInfectedUSB = 1

   UnloadInfectedUSBVirusCount = 5
d. Save the changes and close the file.
e. Open the OfficeScan web console and go to the **Agents** > **Global Agent Settings** screen.
f. Click **Save** to deploy the setting to clients.

   The OfficeScan server deploys the command to OfficeScan clients and adds the following registry entry on all OfficeScan client computers:

Path:
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.\
Key: UnloadInfectedUSB
Type: dword
Value: 1
Key: UnloadInfectedUSBVirusCount
Types: dword
Value: 5 (default value)

Issues resolved by hot fixes for OfficeScan 11.0 Service Pack 1

Hot Fix B3700	Hot Fix B3704	Hot Fix B4965	Hot Fix B4974	Hot Fix B4976	Hot Fix B4977	Hot Fix B4978	Hot Fix B4980
Hot Fix B4983	Hot Fix B4986	Hot Fix B4992	Hot Fix B4993	Hot Fix B4995	Hot Fix B4996	Hot Fix B4999	Hot Fix B5002
Hot Fix B5007.1	Hot Fix B5008	Hot Fix B5009	Hot Fix B5009.1	Hot Fix B5014	Hot Fix B5015	Hot Fix B5016	Hot Fix B5018
Hot Fix B5020	Hot Fix B5024	Hot Fix B5028	Hot Fix B5029	Hot Fix B5030	Hot Fix B5031	Hot Fix B5032	Hot Fix B5033 / 6814
Hot Fix B5037	Hot Fix B5038	Hot Fix B5040	Hot Fix B5042	Hot Fix B5043	Hot Fix B5053	Hot Fix B5057	CP5060
Hot Fix B5066	Hot Fix B5067	Hot Fix B5069	Hot Fix B5070	Hot Fix B5071	Hot Fix B5074	Hot Fix B5077	Hot Fix B5080
Hot Fix B6080	Hot Fix B6082 / CP6155	Hot Fix B6084	Hot Fix B6084.2	Hot Fix B6085	Hot Fix B6088	Hot Fix B6091	Hot Fix B6093
Hot Fix B6094	Hot Fix B6098	Hot Fix B6101	Hot Fix B6103	Hot Fix B6105	Hot Fix B6106	Hot Fix B6109	Hot Fix B6110
Hot Fix B6111	Hot Fix B6112	Hot Fix B6114	Hot Fix B6118	Hot Fix B6120	Hot Fix B6121	CP6125	Hot Fix B6126
Hot Fix B6126.1	Hot Fix B6127	Hot Fix B6128	Hot Fix B6129	Hot Fix B6131	Hot Fix B6133	Hot Fix B6135	Hot Fix B6136
Hot Fix B6138	Hot Fix B6140	Hot Fix B6140.1	Hot Fix B6141	Hot Fix B6147	Hot Fix B6148	Hot Fix B6149	Hot Fix B6151
Hot Fix B6152	Hot Fix B6155	Hot Fix B6157	Hot Fix B6158	Hot Fix B6167	Hot Fix B6167.1	Hot Fix B6168	Hot Fix B6170
Hot Fix B6177	Hot Fix B6178 / 6193	Hot Fix B6181	Hot Fix B6182	Hot Fix B6183	Hot Fix B6185	Hot Fix B6187	CP6196 / 6206
Hot Fix B6196 / CP6206	Hot Fix B6199	Hot Fix B6209	Hot Fix B6212 / 6224	Hot Fix B6213	Hot Fix B6213.1	Hot Fix B6214	Hot Fix B6214.1

Hot Fix B6216	Hot Fix B6217	Hot Fix B6221	Hot Fix B6223	Hot Fix B6231	Hot Fix B6232	Hot Fix B6244	Hot Fix B6250
Hot Fix B6252	Hot Fix B6258	Hot Fix B6263 / 6300	Hot Fix B6267	Hot Fix B6271	Hot Fix B6274	Hot Fix B6277	Hot Fix B6281.1
CP6285	Hot Fix B6292	Hot Fix B6299	Hot Fix B6302	Hot Fix B6306	Hot Fix B6308	Hot Fix B6313	Hot Fix B6315 / 6331
Hot Fix B6317	CP6325	Hot Fix B6325	Hot Fix B6325.1	Hot Fix B6331			

Hot Fix Build 3700 (SBM 347284)

Issue

The OfficeScan agent displays the short detection name on the Virus/Malware Logs.

Solution

This hot fix ensures that the OfficeScan agent displays the long detection name on the Virus/Malware Logs.

Hot Fix Build 3704 (SBM 350759)

Issue

When the OfficeScan server receives multiple policies from a Control Manager 6.0 server, it applies only the first policy.

Solution

This hot fix updates the OfficeScan program to ensure that the OfficeScan server can apply multiple policies from a Control Manager 6.0 server.

Hot Fix Build 4965 (SBM 346778)

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 hot fix improves the speed in which the OfficeScan agent program reports its status to WSC.

Procedure

To apply and deploy the solution globally to shorten the interval of the WSC reporting:

a. Install this hot fix (see Installation) and wait until the new programs deployed to agents.
b. Open the Ofcscan.ini file in the \PCCSRV\ folder in the OfficeScan server installation directory.
c. Add "FirstTimerSystemInterval = 5" under the Global Setting section.

   [Global Setting]

   FirstTimerSystemInterval = 5
d. Save the changes and close the file.
e. Open the OfficeScan web console and go to the **Agents** > **Global Agent Settings** screen.
f. Click **Save** to deploy the setting to all agents.

   The OfficeScan server deploys the command to OfficeScan agents and adds the following registry entry on all OfficeScan agent computers:

   Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

   Key: FirstTimerSystemInterval

   Type: REG_DWORD

   Value: 5
g. Restart the agent computers.

Hot Fix Build 4974 (SBM 346475)

Issue

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

Solution

This hot fix 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".

Hot Fix Build 4976 (SBM 347966)

Issue

Active Directory does not allow some special characters as Active Directory passwords.

Solution

This hot fix ensures that Active Directory can allow special characters as Active Directory passwords.

Hot Fix Build 4977 (SBM 340575)

Issue

There is an interoperability issue between the TMWFP driver and tmeevw service.

Solution

This hot fix removes an unused call out to resolve the interoperability issue.

Hot Fix Build 4978 (SBM 346888)

Enhancement

This hot fix enables OfficeScan Data Loss Prevention™ (DLP) increase the limit of archive file and increase limit of the DLP archive file setting on web console.

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 hot fix updates the "listDeviceInfo.exe" tool to enable it to display information about USB devices when the device information is not in the usual format.

Hot Fix Build 4980 (SBM 344248)

Issue

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

Solution

This hot fix resolves this issue.

Hot Fix Build 4983 (SBM 346475)

Issue

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

Solution

This hot fix 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".

Hot Fix Build 4986 (SBM 347975)

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 hot fix updates the OfficeScan server by preventing queries from accessing the database before the client entry is ready.

Hot Fix Build 4992 (SBM 347260)

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 hot fix updates the "listDeviceInfo.exe" tool to enable it to display information about USB devices when the device information is not in the usual format.

Hot Fix Build 4993 (SBM 347908)

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 hot fix updates the OfficeScan server to display the correct Active Directory domain structure on the Agent Management screen after sorting agents based on Active Directory.

Procedure

To enable the correct grouping of Office agents based on the Active Directory domain structure on the Agent Management screen:

a. Install this hot fix (see Installation).
b. Open the ofcserver.ini file in the \PCCSRV\Private folder on the OfficeScan installation directory.
c. Under the INI_AD_INTEGRATION_SECTION section, add the following key and set its value to "1":

    [INI_AD_INTEGRATION_SECTION]
    IndividualDC = 1

d. Save the changes and close the file.
e. Restart OfficeScan Server Master Service.

Hot Fix Build 4995 (SBM 348589)

Issue

An arithmetic overflow error occurs and triggers the following Microsoft™ Windows™ application even log:

"Arithmetic overflow error converting expression to data type int."

Solution

This hot fix updates the OfficeScan server database process (dbserver.exe) to reverse the order of parameters and prevent the arithmetic overflow event.

Hot Fix Build 4996 (SBM 346332/SBM 344333)

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 hot fix 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.

Hot Fix Build 4999 (SBM 349302)

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 hot fix 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.

Hot Fix Build 5002 (SBM 343440)

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 hot fix allows users to enable the services above by default on a freshly installed OfficeScan agent on the Windows Server platform.

Procedure

To enable the services above in freshly installed OfficeScan agents on the Windows Server platform:

a. Install this hot fix (see Installation).
b. Open the ofcserver.ini file in the \PCCSRV\Private folder of the OfficeScan server.
c. Under INI_SERVER_SECTION, manually add the following keys and set each value to "1".

    [INI_SERVER_SECTION]

    CheckAegisOnServer = 1

    CheckNCIEOnServer = 1

    CheckCCSFOnServer = 1

d. Save the changes and close the file.
e. Open the ofcscan.ini file in the \PCCSRV folder of the OfficeScan server.
f. Under the ServiceSwitch section, find the following keys and set each value to "1".

    [ServiceSwitch]

    EnableAEGISOnServer = 1

    EnableNCIEOnServer = 1

    EnableCCSFOnServer = 1

g. Save the changes and close the file.

Hot Fix Build 5007.1 (SBM 348204)

Enhancement

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

Procedure

To configure the "converter_call_method" setting for DLP and to deploy the setting to OfficeScan agents:

a. Install this hot fix (see Installation).
b. Open the dlp.ini file in the \PCCSRV\Private\ folder on the OfficeScan server.
c. Under the Configure section, manually add the converter_call_method key and set its value to "funccall".

    [Configure]

converter_call_method = funccall

d. Save the changes and close the file.

e. Open the OfficeScan web console and click **Agents** > **Agent Management** > **Select domains or agents** > **Settings** > **DLP settings**.

f. Click **Save** to deploy the settings to agents.

The OfficeScan server deploys the setting to OfficeScan agents and adds the following key in the "dsa.pro" file in the "\Windows\System32\dgagent\" folder:

converter_call_method = funccall

g. Restart all OfficeScan agents.

Hot Fix Build 5008 (SBM 347028)

Issue

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

Solution

The hot fix resolves the DLP blocking issue.

Hot Fix Build 5008 (SBM 344018)

Issue

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

The hot fix resolves the issue by enlarging the queue size to 100,000.

Hot Fix Build 5009 (SBM 345955)

Issue

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

Solution

This hot fix ensures that the ADC detection can successfully work on the network drive.

Hot Fix Build 5009 (SBM 347873)

Issue

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

Solution

This hot fix updates the OfficeScan agent program to ensure that it uploads DLP violation logs to the OfficeScan server normally.

Procedure

To prevent the OfficeScan agent from sending duplicate DLP violation logs upload to the OfficeScan server:

a. Install this hot fix (see Installation).

b. Open the Ofcscan.ini file in the \PCCSRV\ folder on the OfficeScan server installation directory.

c. Under the Global Setting section, manually add the ReindexDLPViolationLog key and set its value to "1".

```
[Global Setting]
ReindexDLPViolationLog = 1
```

> NOTE 🗎 To disable the feature, set "ReindexDLPViolationLog = 0".

d. Save the changes and close the file.

e. Open the OfficeScan web console and go to the **Agents** > **Global Agent Settings** screen.

f. Click **Save** to deploy the setting to agents.

The OfficeScan server deploys the command to OfficeScan agents and adds the following registry entry on all OfficeScan agent computers:

Path:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.

Key: ReindexDLPViolationLog

Type: dword

Value: 1

Hot Fix Build 5009 (SBM 339967)

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.

Procedure

To change the OfficeScan agent permission on an OfficeScan server and to automatically deploy the setting to all OfficeScan agents:

a. Install this hot fix (see Installation).
b. Open the Ofcscan.ini file in the \PCCSRV\ folder on the OfficeScan installation directory.
c. Add the following key under the Global Setting section and set its value to "1".

   [Global Setting]

   PrivilegeContolSetting = 1

> NOTE To disable the full control, set "PrivilegeContolSetting = 0".

d. Save the changes and close the file.
e. Open the OfficeScan web console and go to the **Agents** > **Global Agent Settings** screen.
f. Click **Save** to deploy the setting to agents.

   Path:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc

   Key: PrivilegeContolSetting

   Type: REG_DWORD

   Value: 1

Hot Fix Build 5009.1 (SBM 338933)

Enhancement

This hot fix 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 hot fix, users will be able to configure the agent installation program to automatically uninstall specific third-party antivirus products before installation.

NOTE 🗎 Users can manually add specific third-party antivirus products in "tmpostuninst.ptn" to set the agent installation program to automatically uninstall each.

Procedure

To configure the OfficeScan agent installation program to automatically uninstall specific thirdparty antivirus products:

a. Install this hot fix (see Installation).

b. Open the tmpostuninst.ptn file in the \PCCSRV\Admin folder on the OfficeScan installation directory.

c. Add a section for the specific third-party antivirus product, add the Support key under it, and set its value to "1".

   For example, to enable the agent installation program to remove McAfee™ Agent 5.0.2.132, add the following lines:

   [McAfee Agent 5.0.2.132]

   Support = 1

   NOTE 🗎 To prevent the installation program from automatically removing a program, set "Support = 0".

d. Save the changes and close the file.

Hot Fix Build 5014 (SBM 349806)

Issue

When the OfficeScan server receives multiple policies from a Control Manager 6.0 server, it applies only the first policy.

Solution

This hot fix updates the OfficeScan program to ensure that the OfficeScan server can apply multiple policies from a Control Manager 6.0 server.

Hot Fix Build 5014 (SBM 341617)

Enhancement

This hot fix 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.

NOTE This enhancement requires users to install Control Manager 6.0 hot fix 3359. Contact the Trend Micro Support Team to request for the Control Manager hot fix.

Hot Fix Build 5015 (SBM 345081)

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 hot fix 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.

Hot Fix Build 5016 (SBM 347072)

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 hot fix 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.

Hot Fix Build 5018 (SBM 349429)

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 hot fix ensures that the correct Smart Scan source appears on the "Standard Smart Protection Server List" page.

Hot Fix Build 5020 (SBM 351541)

Issue

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

This hot fix updates the OfficeScan agent program to allow users to set the Scheduled Scan Postpone hour time interval to "12" hours.

Hot Fix Build 5020 (SBM 352232)

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 hot fix 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.

Hot Fix Build 5024 (SBM 351708)

Issue

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

Solution

This hot fix updates the OfficeScan server program files to ensure that VSEncode can decode virus files without issues.

Hot Fix Build 5028 (SBM 352231)

Issue

When users install an OfficeScan agent on a computer running on the 32-bit version of Microsoft™ Windows™ 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 hot fix 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.

Hot Fix Build 5029 (SBM 350647)

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 hot fix updates the BEP module to prevent the high CPU usage issue.

Hot Fix Build 5030 (SBM 352763)

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 hot fix 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.

Hot Fix Build 5031 (SBM 353148/SBM 350647)

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 hot fix updates the BEP module to prevent the high CPU usage issue.

Hot Fix Build 5032 (SBM 353446)

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 hot fix updates the OfficeScan agent program to ensure that the "Resume an interrupted Scheduled Scan" feature works properly.

Hot Fix Build 5033/6184 (SBM 353871/SBM 354760)

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 hot fix 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.

Hot Fix Build 5037 (SBM 354956)

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 hot fix 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.

Hot Fix Build 5038 (SBM 354896)

Issue

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

Solution

This hot fix updates the OfficeScan agent program to improve the way the TmListen service manages the NCIE function.

Hot Fix Build 5038 (SBM 355180)

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 hot fix resolves the memory allocation issue to prevent memory leaks.

Hot Fix Build 5040 (SBM 355334)

Enhancement

This hot fix provides a way for users to enable or disable the Osprey async mode.

Procedure

To enable or disable the Osprey async mode:

a. Install this hot fix (see Installation).

b. Open the ofcscan.ini file in the \PCCSRV folder of the OfficeScan installation directory.

c. Under the Global Setting section, manually add the OspreyAsyncServerLookup key and assign the preferred value.

   [Global Setting]

   OspreyAsyncServerLookup = 0, disables Osprey async mode

   OspreyAsyncServerLookup = 1, enables Osprey async mode

d. Save the changes and close the file.

e. Open the OfficeScan web console and go to the **Agents** > **Global Agent Settings** screen.

f. Click **Save** to deploy the setting to agents.

   The OfficeScan server deploys the command to OfficeScan agents and adds the following registry entry on all OfficeScan agent computers:

   Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey\Scan\Common\HttpManager\config

   Key: AsyncServerLookup

   Type: dword

   Value: 0, 1

g. Restart OfficeScan agents.

Hot Fix Build 5042 (SBM 345393)

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 hot fix 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.

Procedure

To disable the self-protection feature of the AEGIS module in affected computers:

a. Install this hot fix (see Installation).

b. Open the ofcscan.ini file in the \PCCSRV\ folder of the OfficeScan installation directory.

c. Under the Global Setting section, add the following key and set its value to "1".

   [Global Setting]

   SkipDuplicateSameAccess = 1

d. Save the changes and close the file.

e. Open the OfficeScan server management console and go to **Agents** > **Global Agent Settings**.

f. Click **Save** to deploy the setting to all clients.

g. Restart the OfficeScan client.

   The OfficeScan client program automatically installs the following registry key:

   Path:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tmactmon\Parameters

   Key: SkipDuplicateSameAccess

   Type: dword

   Value: 1, disables the self-protection feature; 0, enables the self-protection feature

Hot Fix Build 5043 (SBM 356053)

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 hot fix 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.

Procedure

To disable the self-protection feature of the AEGIS module in affected computers:

a. Install this hot fix (see Installation).

b. Open the ofcscan.ini file in the \PCCSRV\ folder of the OfficeScan installation directory.

a. Under the Global Setting section, add the following key and set its value to "1".

   [Global Setting]

   SkipDuplicateSameAccess = 1

b. Save the changes and close the file.

c. Open the OfficeScan server management console and go to **Agents** > **Global Agent Settings**.

d. Click **Save** to deploy the setting to all clients.

e. Restart the OfficeScan client.

   The OfficeScan client program automatically installs the following registry key:

   Path:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tmactmon\Parameters

   Key: SkipDuplicateSameAccess

   Type: dword

   Value: 1, disables the self-protection feature; 0, enables the self-protection feature

Hot Fix Build 5053 (SBM 354095)

Issue

The firewall details page of the OfficeScan client console does not refresh automatically after the security level setting changes.

Solution

This hot fix updates the OfficeScan agent program to ensure that the firewall details page of the OfficeScan client console refreshes automatically when the security level setting changes.

Hot Fix Build 5053 (SBM 356053)

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 hot fix 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.

Procedure

To disable the self-protection feature of the AEGIS module in affected computers:

a. Install this hot fix (see Installation).
b. Open the ofcscan.in file in the "\PCCSRV\ folder of the OfficeScan installation directory.
c. Under the Global Setting section, add the following key and set its value to "1".

   [Global Setting]

   SkipDuplicateSameAccess = 1
d. Save the changes and close the file.
e. Open the OfficeScan server management console and go to **Agents** > **Global Agent Settings**.
f. Click **Save** to deploy the setting to all clients.
g. Restart the OfficeScan client.

   The OfficeScan client program automatically installs the following registry key:

   Path:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tmactmon\Parameters

   Key: SkipDuplicateSameAccess

   Type: dword

   Value: 1, disables the self-protection feature; 0, enables the self-protection feature

Hot Fix Build 5053 (SBM 354020)

Enhancement

This hot fix enables OfficeScan Data Loss Prevention™(DLP)increase the limit of archive file and increase limit of the DLP archive file setting on web console.

Hot Fix Build 5057 (SBM 354124)

Issue

Automatic agent grouping uses rules defined by Microsoft™ Windows™ Active Directory (AD) domains. Sometimes, after the OfficeScan server synchronizes AD information from the Windows server, the status of enabled grouping rules shows a "Warning" sign.

Solution

This hot fix updates the OfficeScan programs to ensure that the enabled grouping rules will not be effected by the synchronized AD information.

Critical Patch 5060 (SBM 357850)

Issue

OfficeScan leaks encrypted account passwords during web console operations. Unauthorized users could use the leaked encrypted password to log on to the OfficeScan server console.

Solution

This critical patch ensures that OfficeScan does not leak encrypted passwords.

Hot Fix Build 5066 (SBM 357507)

Issue

The Microsoft™ Windows™ Event Log generates too many messages.

Solution

This hot fix enables OfficeScan to extend the cache time to 12 hours.

Hot Fix Build 5067 (SBM 358603)

Enhancement

This hot fix improves the checking mechanism of the OfficeScan agent program to protect the Smart Scan Agent Pattern and Virus Pattern files in endpoints from corruption.

Hot Fix Build 5069 (SBM 355701)

Issue

An initialized issue related to the OfficeScan Control Manager Agent service ("OfcCMAgent.exe") may cause the OfcCMAgent.exe to stop unexpectedly.

Solution

This hot fix updates the OfficeScan Control Manager Agent program to prevent from this issue.

Hot Fix Build 5070 (SBM 359313)

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 hot fix 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.

Hot Fix Build 5071 (SBM 357054)

Issue

When there are hot fix updates, the OfficeScan server checks all client components and prompts all clients with old hot fix versions to apply the updates including those where the No Program Upgrade option is enabled. This triggers a large number of unnecessary client notifications.

Solution

This hot fix ensures that the OfficeScan server does not notify a client of hot fix updates if the No Program Upgrade option is enabled in the client.

Hot Fix Build 5074 (SBM 358532)

Issue

When an unreachable OfficeScan agent reports its onstart status to the OfficeScan server, the server does not automatically set the updateflag for the agent. As a result, the agent will not receive updates until after a file change event on the OfficeScan server.

Solution

This hot fix enables the OfficeScan server to set the updateflag of unreachable OfficeScan agents automatically once it receive the onstart status of the agents.

Hot Fix Build 5077 (JIRA 3129)

Issue

Sometimes, the value of the "SourceUUID" setting in the "Ofcserver.ini" file is overwritten which prevents OfficeScan from updating the suspicious object list.

Solution

This hot fix ensures that the "SourceUUID" setting is not overwritten unexpectedly.

Hot Fix Build 5080 (JIRA 2745)

Issue

The Vulnerability Scanner may attempt to access an invalid file path which triggers blue screen of death (BSOD) on computers running Microsoft™ Windows™ Vista™ or any version released after it, for example, Windows Server 2008 and later versions.

Solution

This hot fix updates the Vulnerability Scanner to prevent it from attempting to access invalid file paths.

Hot Fix Build 6080 (SBM 329424/SBM 330041/SBM 330554)

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.

Hot Fix Build 6082/Critical Patch 6155 (SBM 347481/SBM 352702)

Issue

A handle leak issue that may occur while the OfficeScan server handles the "ofcserver.ini" file may corrupt the file.

Solution

This hotfix resolves the issue by ensuring that the OfficeScan server handles the INI properly.

Hot Fix Build 6084 (SBM 347525)

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.

Hot Fix Build 6084.2 (SBM 348437)

Issue

OfficeScan continues to scan network drives even if the "Scan network drive" setting is disabled in Real-time Scan.

Solution

This hot fix ensures that OfficeScan correctly implements the "Scan network drive" setting when performing Real-time Scan.

Hot Fix Build 6084.2 (SBM 347284)

Issue

The OfficeScan agent displays the short detection name on the Virus/Malware Logs.

Solution

This hot fix ensures that the OfficeScan agent displays the long detection name on the Virus/Malware Logs.

Hot Fix Build 6085 (SBM 347807)

Issue

Data Loss Prevention™ Endpoint causes a Blue Screen of Death (BSoD) on Windows™ 10 Red Stone 1.

Solution

This hot fix resolves the BSoD issue on Windows™ 10 Red Stone 1.

Hot Fix Build 6088 (SBM 348887)

Issue

When using the Microsoft™ 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 hot fix uses another method when handling the SQL schema update instead of using the Windows application program interface (API), which resolves this issue.

Enhancement

This hot fix enhances the OfficeScan folder write permission check before doing the SQL migration. End users should grant Windows domain users full control permissions to the OfficeScan server folder and include inheritable permissions from the parent of this object by local administrator or Active Directory (AD) build-in administrator.

Hot Fix Build 6091 (SBM 348682)

Issue

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

Solution

This hot fix ensures that the OfficeScan Update Agent deploys the Suspicious Connection Settings to OfficeScan clients.

Hot Fix Build 6093 (SBM 348911)

Enhancement

This hot fix enables DLP Endpoint SDK 6.0 to support Chrome™ 51.0.2704.106m with QUIC enabled.

Hot Fix Build 6094 (SBM 347090)

Issue

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

Solution

This hot fix 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.

Hot Fix Build 6098 (SBM 348679)

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 predefined multilayer domains.

Procedure

To assign an agent to a multilayered domain that has been pre-defined in the agent computer before agent installation:

a. Install this hot fix (see "Installation").
b. Open Windows Registry Editor on agent machine.
c. Add following registry information using the information of the preferred domain:
   For 32-bit OfficeScan agents:
   [HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorpOnce\

CurrentVersion]

"Domain"="domain_name"

"Server"="server_name"

"ServerPort"=dword:xxxxxxxx

[HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorpOnce\CurrentVersion\Internet Settings]

"ServerPort"=dword:xxxxxxxx

"Server"="server_name"

"UseProxy"=dword:00000000

For 64-bit OfficeScan agents:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorpOnce\CurrentVersion]

"Domain"="domain_name"

"Server"="server_name"

"ServerPort"=dword:xxxxxxxx

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorpOnce\CurrentVersion\Internet Settings]

"ServerPort"=dword:xxxxxxxx

"Server"="server_name"

"UseProxy"=dword:00000000

d. Install the OfficeScan agent.

> NOTE Users have to wait until the next day to perform browser-based agent installation.

Since agent packages for browser-based installation are created daily at 1AM, users will need to wait until the next day after installing this hot fix to be able to perform browser-based agent installation.

Hot Fix Build 6101 (SBM 349224)

Issue

The OfficeScan exclusion list does not work on mount points; drives that are mapped as folders to an existing file system.

Solution

This hot fix ensures that OfficeScan clients receive the complete list of approved devices to ensure that the exclusion list works normally.

Hot Fix Build 6103 (SBM 348995)

Issue

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

Solution

This hot fix ensures that all the information on the page are translated correctly.

Hot Fix Build 6105 (SBM 348521)

Enhancement

This hot fix 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.

Procedure

To add the "Offline Time" column to the Agent Management tree:

a. Install this hot fix (see "Installation").

b. Open the "ofcserver.ini" file in the "\PCCSRV\private\" folder on the OfficeScan server.

c. Add the "ShowNotConnectedTime" key under the "SERVER_CONSOLE_SECTION" section and set its value to "1".

```
[SERVER_CONSOLE_SECTION]
ShowNotConnectedTime = 1
```

> NOTE To hide the "Offline Time" column in the Agent Management tree, set "ShowNotConnectedTime = 0".

d. Reload or reopen the web browser.

Hot Fix Build 6106 (SBM 350909)

Issue

The scan action information that appears in the Control Manager console does not match the information in OfficeScan logs.

Solution

This hot fix ensures that the OfficeScan server sends the correct scan action results to Control Manager so that the information in the Control Manager console matches the information on OfficeScan logs.

Hot Fix Build 6109 (SBM 349291/SBM 349315)

Enhancement

This hot fix upgrades the Web Blocking Service module to support IP lookup when there are no results for URL lookup.

Hot Fix Build 6110 (SBM 347260)

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 hot fix updates the "listDeviceInfo.exe" tool to enable it to display information about USB devices when the device information is not in the usual format.

Hot Fix Build 6111 (SBM 343705)

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 hot fix resolves the memory allocation issue to prevent memory leaks.

Hot Fix Build 6112 (SBM 349873)

Issue

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

This hot fix 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.

Hot Fix Build 6112 (SBM 349169)

Issue

Some privilege issues occur when DRE attempts to access a file on a UNC path that breaks the existing UNC path connection.

Solution

This hot fix ensures that the OfficeScan DRE feature works normally on UNC paths.

Hot Fix Build 6114 (SBM 349491)

Issue

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

Solution

This hot fix updates the server program to ensure that users can access the pages normally.

Hot Fix Build 6118 (SBM 343900)

Issue

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

Solution

This hot fix ensures that the corresponding DLP violation logs refers to the correct channel.

Hot Fix Build 6118 (SBM 346362)

Issue

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

Solution

This hot fix ensures that only users with the correct application permission can run applications under USB storage devices.

Hot Fix Build 6120 (SBM 349937/SBM 346965)

Issue

The OfficeScan server sends configuration change notifications to OfficeScan agents twice.

Solution

This hot fix ensures that the OfficeScan server sends only one notification for each set of configuration changes to OfficeScan agents.

Hot Fix Build 6120 (SBM 349937/SBM 347908)

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 hot fix updates the OfficeScan server to display the correct Active Directory domain structure on the Agent Management screen after sorting agents based on Active Directory.

Procedure

To enable the correct grouping of Office agents based on the Active Directory domain structure on the Agent Management screen:

a. Install this hot fix (see "Installation").

b. Open the "ofcserver.ini" file in the "\PCCSRV\Private" folder on the OfficeScan installation directory.

c. Under the "INI_AD_INTEGRATION_SECTION" section, add the following key and set its value to "1":

    [INI_AD_INTEGRATION_SECTION]

    IndividualDC = 1

d. Save the changes and close the file.

e. Restart OfficeScan Server Master Service.

Hot Fix Build 6121 (SBM 345044)

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 hot fix ensures that the OfficeScan agent properly unregisters from its original OfficeScan server if a connection issue occurs.

Procedure

a. Install this hot fix (see "Installation").

b. Open the " ofcserver.ini" file in the "\PCCSRV\Private" folder of the OfficeScan installation directory.

c. Add the following section and key.

    [MOVE_CLIENT_SECTION]

    EnableDeleteAfterMove = 1

d. Save the changes and close the file.

e. Restart the OfficeScan Master Service.

Critical Patch 6125

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).

Hot Fix Build 6126 (SBM 350139)

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 hot fix 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.

Hot Fix Build 6126.1 (SBM 349445)

Issue

When users attempt to register OfficeScan to a Trend Micro Control Manager™ server that communicates using Transport Layer Security (TLS) 1.2, the registration fails and users encounter an error on the Control Manager console.

Solution

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

Hot Fix Build 6127 (SBM 350116)

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 hot fix extends the timeout value to ten (10) minutes, which allows the OfficeScan server to display the results of the Advanced Search results successfully.

Hot Fix Build 6128 (SBM 347348)

Enhancement

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

Enhancement

This hot fix 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.

Procedure

To enable and configure this Enhancement:

a. Install this hot fix (see "Installation").
b. Open the "Ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan server installation directory.
c. Under the "Global Setting" section, manually add the "ProtectionReportFrequency" and "AutoOnStart" keys and set the preferred value for each.

   [Global Setting]

   ProtectionReportFrequency = (the frequency in minutes at which the server should check if a client's UID is in the database through a compliance report, the minimum value is 2 minutes)

   AutoOnStart

   = 1, enables the OfficeScan server to trigger an onstart command to agents to register back to the server if it cannot find the agent's UID in the database

   = 0, disables the command trigger
d. Save the changes and close the file.
e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.
f. Click "Save" to deploy the setting to agents.

The OfficeScan server deploys the command to OfficeScan agents and adds the following registry entries on all OfficeScan agent computers:

Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

Key: ProtectionReportFrequency

Type: REG_DWORD

Value: 2

Key: AutoOnStart

Type: REG_DWORD

Value: 1

Hot Fix Build 6129 (SBM 347282/SBM 349815)

Enhancement

This hot fix adds a way to configure OfficeScan clients to skip digital signature checking of OfficeScan client program files while downloading hot fix files and reloading the scan engine.

Procedure

To prevent OfficeScan clients from checking the digital signature of program files while downloading hot fix files and reloading the scan engine:

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder of the OfficeScan installation directory.
c. Under the "Global Setting" section, add the following key and set its value to "1".

    [Global Setting]

    DOVF = 1

d. Save the changes and close the file.
e. Open the OfficeScan server management console and go to "Agents > Global Agent Settings".
f. Click "Save" to deploy the setting to all clients.
g. Restart the OfficeScan client.

The OfficeScan client program automatically installs the following registry key:

Path:

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

Key: DOVF

Value: 1

Hot Fix Build 6131 (SBM 351400)

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 hot fix resolves this issue by updating the OpenSSL component of the server module and Smart Scan common module.

Hot Fix Build 6133 (SBM 349682)

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 hot fix 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.

Hot Fix Build 6135 (SBM 351716)

Issue

BSOD occurs when the firewall rule has too many filters.

Solution

This hot fix updates the Network Security Components to prevent the BSOD issue.

> NOTE 🗎 OfficeScan client computers should be restarted immediately after installing this hot fix to be able to use the newly-deployed NSC modules.

Hot Fix Build 6135 (SBM 349382/SBM 349804)

Enhancement

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

Hot Fix Build 6136 (SBM 351424)

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.

Hot Fix Build 6138 (SBM 351092)

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 hot fix makes the comparison mechanism case-insensitive to ensure that users can accurately assess endpoints.

Hot Fix Build 6140 (SBM 351523)

Issue

Several duplicate entries appear in the Behavior Monitoring Exclusion List.

Solution

This hot fix disables the "Save" button on the page immediately after users click on it.

Hot Fix Build 6140.1 (SBM 349969)

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 hot fix updates the agent remote installation process to ensure that it removes the mapped network drivers automatically after agent installation.

Hot Fix Build 6141 (SBM 348733)

Issue

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

Solution

This hot fix ensures that the DLP module can block attachments with sensitive information in Outlook™ Web App 2003 and 2010.

Hot Fix Build 6141 (SBM 348919)

Issue

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

This hot fix prevents the high disk space usage issue.

Hot Fix Build 6147 (SBM 352003)

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 hot fix 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.

Hot Fix Build 6148 (SBM 351433)

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 hot fix updates the server program to ensure that it reads the WRS flag from the "ofcscan.ini" file.

Hot Fix Build 6149 (SBM 352606)

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 hot fix enables the Ransomware Widget to include ransomware detection logs that start with "Ransom." in the ransomware count.

Hot Fix Build 6151 (SBM 352084)

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 hot fix allows users to enable the services above by default on a freshly installed OfficeScan agent on the Windows Server platform.

Procedure

To enable the services above in freshly installed OfficeScan agents on the Windows Server platform:

a. Install this hot fix (see "Installation").
b. Open the "ofcserver.ini" file in the "\PCCSRV\Private" folder of the OfficeScan server.
c. Under the "INI_SERVER_SECTION", manually add the following keys and set each value to "1".

    [INI_SERVER_SECTION]
    CheckAegisOnServer = 1
    CheckNCIEOnServer = 1
    CheckCCSFOnServer = 1

d. Save the changes and close the file.
e. Open the "ofcscan.ini" file in the "\PCCSRV"folder of the OfficeScan server.
f. Under the "ServiceSwitch" section, find the following keys and set each value to "1".

    [ServiceSwitch]
    EnableAEGISOnServer = 1
    EnableNCIEOnServer = 1
    EnableCCSFOnServer = 1

g. Save the changes and close the file.

Hot Fix Build 6152 (SBM 350056)

Issue

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

Solution

This hot fix updates the OfficeScan agent program to ensure that the DLP module can update successfully.

Hot Fix Build 6155 (SBM 352702)

Issue

A handle leak issue that may occur while the OfficeScan server handles the "ofcserver.ini" file may corrupt the file.

Solution

This hot fix resolves the issue by ensuring that the OfficeScan server handles the INI properly.

Hot Fix Build 6157 (SBM 351733)

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 hot fix resolves the issue by updating the OfficeScan Common Client Solution Framework module in OfficeScan 11.0 Service Pack 1.

Hot Fix Build 6158 (SBM 352281)

Issue

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

Solution

This hot fix updates OfficeScan agent program to prevent the high CPU usage issue.

Hot Fix Build 6167 (SBM 352149)

Issue

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

Solution

This hot fix updates the OfficeScan agent program to ensure that "Ntrtscan.exe" starts and works normally.

Hot Fix Build 6167 (SBM 352050)

Enhancement

This hot fix 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 hot fix, users will be able to configure the agent installation program to automatically uninstall specific third-party antivirus products before installation.

> NOTE 🗎 Users can manually add specific third-party antivirus products in "tmpostuninst.ptn" to set the agent installation program to automatically uninstall each.

Procedure

To configure the OfficeScan agent installation program automatically uninstall specific third-party antivirus products:

a. Install this hot fix (see "Installation").

b. Open the "tmpostuninst.ptn" file in the "\PCCSRV\Admin" folder on the OfficeScan installation directory.

c. Add a section for the specific third-party antivirus product, add the "Support" key under it, and set its value to "1". For example, to enable the agent installation program to remove McAfee™ Agent 5.0.2.132, add the following lines:

```
[McAfee Agent 5.0.2.132]
Support = 1
```

NOTE To prevent the installation program from automatically removing a program, set "Support = 0".

d. Save the changes and close the file.

Hot Fix Build 6167 (SBM 352245)

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.

Procedure

To change the OfficeScan agent permission on an OfficeScan server and to automatically deploy the setting to all OfficeScan agents:

a. Install this hot fix (see "Installation").

b. Open the "Ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan installation directory.

c. Add the following key under the "Global Setting" section and set its value to "1".

[Global Setting]

PrivilegeContolSetting = 1

NOTE To disable the full control, set "PrivilegeContolSetting = 0".

d. Save the changes and close the file.

e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.

f. Click "Save" to deploy the setting to agents.

Path: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc

Key: PrivilegeContolSetting

Type: REG_DWORD

Value: 1

Hot Fix Build 6167.1 (SBM 350646)

Enhancement

OfficeScan and Data Loss Prevention(DLP) starts support multiple forensic data session in the violation logs.

Hot Fix Build 6168 (SBM 352886)

Issue 1

When users use "http://dlptest.com" to test the DLP policy, the OfficeScan agent does not block illegal information on the website.

Solution 1

This hot fix ensures that the DLP module of OfficeScan agents blocks HTP/HTTPS posts in websites that contain illegal information.

Issue 2

An issue in the DLP module triggers a high CPU usage issue related to "SourceTree.exe".

Solution 2

This hot fix resolves the issue in the DLP module to prevent the high CPU usage issue.

Issue 3

The DLP data identifiers expression "UK - RD&E Hospital Number" algorithm may trigger some false alarms.

Solution 3

This hot fix updates the "UK - RD&E Hospital Number" algorithm to help avoid false alarms.

Issue 4

DLP causes Google™ Chrome™ to stop responding while users upload an attachment to Gmail by the drag and drop method.

Solution 4

This hot fix ensures that users can drag and drop file attachments in Gmail on Google™ Chrome™.

Enhancement 1

This hot fix enables DLP Endpoint SDK 6.0 to support version 53.0.2785.116 m of the Google™ Chrome™ web browser but not its QUIC mode.

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.

Procedure

To change the OfficeScan agent permission on an OfficeScan server and to automatically deploy the setting to all OfficeScan agents:

a. Install this hot fix (see "Installation").
b. Open the "Ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan installation directory.
c. Add the following key under the "Global Setting" section and set its value to "1".

   [Global Setting]

   PrivilegeContolSetting = 1

   NOTE 🗎 To disable the full control, set "PrivilegeContolSetting = 0".

d. Save the changes and close the file.
e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.
f. Click "Save" to deploy the setting to agents.

   Path: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc

   Key: PrivilegeContolSetting

   Type: REG_DWORD

   Value: 1

Hot Fix Build 6170 (SBM 353233)

Issue

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

Solution

This hot fix resolves the issue by updating the OfficeScan server program to ensure that the OfficeScan server syncs up with the AD domain properly.

Hot Fix Build 6177 (SBM 352580)

Enhancement

This hot fix provides a way for users to enable or disable the Osprey async mode.

Procedure

a. Install this hot fix (see "Installation").

b. Open the "ofcscan.ini" file in the "\PCCSRV" folder of the OfficeScan installation directory.

g. Add the key in the "Global Setting" section and assign the preferred value.

[Global Setting]

OspreyAsyncServerLookup

= 0, disables Osprey async mode

=1, enables Osprey async mode

c. Save the changes and close the file.

d. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.

e. Click "Save" to deploy the setting to agents.

The OfficeScan server deploys the command to OfficeScan agents and adds the following registry entry on all OfficeScan agent computers:

Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey\Scan\Common\HttpManager\config

Key: AsyncServerLookup

Type: dword

Hot Fix Build 6178/6193 (SBM 352548/SBM 353384)

Issue

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

Solution

This hot fix updates the OfficeScan agent program to prevent the abnormal messages in computers running on the Windows™ 10 Red Stone 1 platform.

Hot Fix Build 6178/6193 (SBM 353648/SBM 354503/SBM 354563/SBM 354690)

Issue

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

Solution

This hot fix updates an agent file to ensure that the OfficeScan agent can scan files specified using UNC paths successfully.

Hot Fix Build 6181 (SBM 353986)

Enhancement

This hot fix 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.

Procedure

To enable and configure this Enhancement:

a. Install this hot fix (see "Installation").
b. Open the "Ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan server installation directory.
c. Under the "Global Setting" section, manually add the "ProtectionReportFrequency" and "AutoOnStart" keys and set the preferred value for each.

    [Global Setting]

    ProtectionReportFrequency = (the frequency in minutes at which the server should check if a client's UID is in the database through a compliance report, the minimum value is 2 minutes)

AutoOnStart

= 1, enables the OfficeScan server to trigger an onstart command to agents to register back to the server if it cannot find the agent's UID in the database

= 0, disables the command trigger

d. Save the changes and close the file.
e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.
f. Click "Save" to deploy the setting to agents.

The OfficeScan server deploys the command to OfficeScan agents and adds the following registry entries on all OfficeScan agent computers:

Path:HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.
Key: ProtectionReportFrequency
Type: REG_DWORD
Value: 2
Key: AutoOnStart
Type: REG_DWORD
Value: 1

Hot Fix Build 6181 (SBM 353986)

Enhancement

This hot fix adds a way to configure OfficeScan clients to skip digital signature checking of OfficeScan client program files while downloading hot fix files and reloading the scan engine.

Procedure

To prevent OfficeScan clients from checking the digital signature of program files while downloading hot fix files and reloading the scan engine:

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder of the OfficeScan installation directory.
c. Under the "Global Setting" section, add the following key and set its value to "1".

[Global Setting]
DOVF = 1

d. Save the changes and close the file.

e. Open the OfficeScan server management console and go to "Agents > Global Agent Settings".

f. Click "Save" to deploy the setting to all clients.

g. Restart the OfficeScan client.

The OfficeScan client program automatically installs the following registry key:

Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

Key: DOVF

Value: 1

Hot Fix Build 6182 (SBM 353787)

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 hot fix updates the OfficeScan agent program to ensure that OfficeScan agents upload firewall logs only when enabled to do so.

Hot Fix Build 6183 (SBM 349599)

Enhancement

This hot fix improves the checking mechanism of the OfficeScan agent program to protect the Smart Scan Agent Pattern and Virus Pattern files in endpoints from corruption.

Hot Fix Build 6185 (SBM 355732)

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 hot fix updates the ActiveUpdate module to ensure that the OfficeScan agent can successfully update its pattern files from the OfficeScan server.

Procedure

To ensure that the OfficeScan agent can successfully update its pattern files from the OfficeScan server:

a. Install this hot fix (see "Installation").
b. Open the "Ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan server installation directory.
c. Under the "Global Setting" section, manually add the "CheckDigitalSignatureForUpgrade" key and set its value to "0".

    [Global Setting]

    CheckDigitalSignatureForUpgrade = 0

> NOTE To disable the feature, set "CheckDigitalSignatureForUpgrade = 1".

d. Save the changes and close the file.
e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.
f. Click "Save" to deploy the setting to agents.

The OfficeScan server deploys the command to OfficeScan agents and adds the following registry entry on all OfficeScan agent computers:

Path: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\
PC-cillinNTCorp\CurrentVersion\Misc.
Key: CheckDigitalSignatureForUpgrade
Type: dword
Value: 0

Hot Fix Build 6187 (SBM 354226)

Issue

OfficeScan Data Protection causes Google™ Chrome™ version 53.0.2785.116 hang.

Solution

This hot fix resolves the hang issue when Chrome™ is running on its QUIC mode.

Critical Patch 6196/Critical Patch 6206

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 critical patch 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.

Hot Fix Build 6196/Critical Patch 6206 (SBM 352967)

Issue

Some drivers cannot be loaded in Microsoft™ Windows™ 10 when both UEFI and Secure Boot are enabled.

Solution

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

Hot Fix Build 6196/Critical Patch 6206 (SBM 353712)

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 hot fix 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.

Procedure

To disable the self-protection feature of the AEGIS module in affected computers:

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder of the OfficeScan installation directory.
c. Under the "Global Setting" section, add the following key and set its value to "1".

    [Global Setting]

    SkipDuplicateSameAccess = 1
d. Save the changes and close the file.
e. Open the OfficeScan server management console and go to "Agents > Global Agent Settings".
f. Click "Save" to deploy the setting to all clients.
g. Restart the OfficeScan client.

The OfficeScan client program automatically installs the following registry key:

PATH: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tmactmon\Parameters

KEY: SkipDuplicateSameAccess

TYPE: dword

VALUE: 1, disables the self-protection feature

0, enables the self-protection feature

Hot Fix Build 6196/Critical Patch 6206 (SBM 354440)

Issue

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

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

Hot Fix Build 6199 (SBM 353736)

Enhancement

This hot fix improves the index mechanism for the SQL table containing the OfficeScan agent information.

Hot Fix Build 6209 (SBM 353132)

Issue

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

Solution

This hot fix ensures that the "Update Information" button works normally and that the correct license information appears on the OfficeScan "Product License" page.

Hot Fix Build 6212/6224 (SBM 352273/SBM 356025)

Issue

The UMH driver triggers an unexpected error.

Solution

This hot fix updates the UMH driver to resolve the issue.

Hot Fix Build 6212/6224 (SBM 351585)

Issue

The UMH driver triggers an unexpected error in the Windows™ 10 Red Stone 1 platform.

Solution

This hot fix updates the UMH driver to resolve the issue.

Hot Fix Build 6213 (SBM 355509)

Issue

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

Solution

This hot fix 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.

Hot Fix Build 6213.1 (SBM 352977)

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 hot fix ensures that when the "PolicyExportTool.exe" utility exports OfficeScan policies from Control Manager™, the exported policies display the correct component types.

Hot Fix Build 6214 (SBM 353505)

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 hot fix corrects the "Date/Time" information on the "Spyware/Grayware Log" page.

Hot Fix Build 6214.1 (SBM 355109)

Issue

The "Unmanaged Endpoints" page of the OfficeScan web console may not display the progress of the agent installation task if a selected endpoint under the Active Directory (AD) contains an ampersand character "&".

Solution

This hot fix ensures that the "Unmanaged Endpoints" page displays the progress of the agent installation task.

Hot Fix Build 6216 (SBM 350316)

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 hot fix 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.

Procedure

To disable the self-protection feature of the AEGIS module in affected computers:

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder of the OfficeScan installation directory.
c. Under the "Global Setting" section, add the following key and set its value to "1".

    [Global Setting]

    SkipDuplicateSameAccess = 1
d. Save the changes and close the file.
e. Open the OfficeScan server management console and go to "Agents > Global Agent Settings".
f. Click "Save" to deploy the setting to all clients.
g. Restart the OfficeScan client.

The OfficeScan client program automatically installs the following registry key:

PATH: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tmactmon\Parameters

KEY: SkipDuplicateSameAccess

TYPE: dword

VALUE: 1, disables the self-protection feature

0, enables the self-protection feature

Hot Fix Build 6217 (SBM 355734)

Issue

The "dsu_convert.exe" tool stops unexpectedly and triggers an error message when it encounters multibyte characters in the "DomainSetting.ini" file.

Solution

This hot fix resolves this issue by enabling the "dsu_convert.exe" tool to support multibyte characters.

Hot Fix Build 6221 (SBM 355317)

Issue

Setting "RmvTmTDI = 1" removes the following OfficeScan agent drivers which can trigger WRS to stop working.

- TMTDI.sys
- TMEEVW.sys
- TMUSA.sys

Solution

This hot fix provides a new option that allows users to prevent OfficeScan from removing the "TMEEVW.sys" and "TMUSA.sys" drivers when "RmvTmTDI" is enabled to ensure that WRS still works normally under this scenario.

Procedure

To enable OfficeScan to remove only the "TMTDI.sys" driver when "RmvTmTDI = 1":

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder of the OfficeScan installation directory.
c. Under the "Global Setting" section, add the following key and set its value to "1".

    [Global Setting]
    RmvTmTDI = 1
    KeepOspreyWhenRmvTmTDI = 1

d. Save the changes and close the file.

e. Open the OfficeScan server management console and go to "Agents > Global Agent Settings".

f. Click "Save" to deploy the setting to all clients.

g. Restart the OfficeScan client.

The OfficeScan client program automatically installs the following registry key:

PATH: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.
KEY: KeepOspreyWhenRmvTmTDI
TYPE: DWORD
VALUE: 1

Hot Fix Build 6223 (SBM 349600)

Enhancement

This hot fix adds settings for the following OfficeScan services on the domain level of Windows server platforms.

- Behavior Monitoring Service
- Firewall Service
- Trend Micro Data Loss Prevention™ (DLP) Service
- Suspicious Connection Service
- Advanced Protection Service

Procedure

To enable the new service settings:

a. Install this hot fix (see "Installation").

b. Open the "ofcserver.ini" file in the "\PCCSRV\Private" folder on the OfficeScan installation directory.

a. Under the "INI_SERVER_SECTION" section, manually add the following key and set its value to "1".

[INI_SERVER_SECTION]

SupportToConfigureServerPlatformForMultiClient = 1

c. Save the changes and close the file.

Hot Fix Build 6231 (SBM 354728)

Enhancement

This hot fix provides a way for users to configure OfficeScan agents to automatically disconnect an established connection and to re-establish a connection when the network isolation feature is triggered from a Control Manager server.

Procedure

To enable the new service settings:

a. Install this hot fix (see "Installation").

b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan installation directory.

c. Under the "Global Setting" section, manually add the following key and set its value to "1".

[Global Setting]

cnqConnectionTermination = 1

d. Save the changes and close the file.

e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.

f. Click "Save" to deploy the setting to clients.

Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

Key: cnqConnectionTermination

Type: DWORD

Value:

0 = OfficeScan does not support network re-establish

1 = OfficeScan supports network re-establish

NOTE 🗎 This function works only on computers that retrieve its IP address from the DHCP server automatically.

Hot Fix Build 6232 (SBM 354983)

Issue

AutoCAD™ closes unexpectedly after users enable the Trend Micro Data Loss Prevention™ function on computers protected by OfficeScan Agent.

Solution

This hot fix adds AutoCAD into the approved list to ensure that it works normally on computers protected OfficeScan Agent while the Data Loss Prevention™ function is enabled.

Hot Fix Build 6232 (SBM 355208)

Issue

Boot2Docker does not launch on Windows 7/10 when users enable the Trend Micro Data Loss Prevention™.

Solution

This hot fix ensures that Boot2Docker works normally on Windows 7/10 computers protected OfficeScan Agent while the Data Loss Prevention™ function is enabled.

Hot Fix Build 6232 (SBM 343900)

Issue

Users can delete files under USB storage devices that they only have READ permission to access.

Solution

This hot fix ensures that only users with the correct application permission can run applications under USB storage devices.

Hot Fix Build 6232 (SBM 356408)

Enhancement

This hot fix enables Data Loss Prevention™ Endpoint SDK 6.0 starts to support Google™ Chrome™ version 54.0.2840.99.

Hot Fix Build 6244 (SBM 349527)

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 hot fix ensures that the pop-up window correctly indicates that the malware has been "detected".

Hot Fix Build 6250 (SBM 356853)

Issue

Installing OfficeScan 10.5 Patch 6 by web installation also installs ActiveX on the computer, however, ActiveX uninstallation. As a result, users encounter an error is not removed during client while installing OfficeScan 11 Service Pack 1 Critical Patch 6054 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 hot fix ensures that the OfficeScan server adds the version information of the "WinNTChk.cab" file when it triggers web installation.

Hot Fix Build 6252 (SBM 357563)

Issue

It is reported that the OfficeScan NT Listener service (TmListen.exe) in OfficeScan 11.0 Service Pack 1 Patch 1 failed to start up on endpoints running Microsoft™ Windows™ Vista or Windows Server 2008.

Solution

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

Hot Fix Build 6252 (SBM 352284)

Issue

The User Mode Hooking (UMH) driver causes an unexpected error.

Solution

This hot fix updates the UMH driver to resolve this issue.

Hot Fix Build 6252 (SBM 357381)

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 hot fix 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.

Hot Fix Build 6252 (SBM 355584)

Issue

In some OfficeScan agents managed by the Update Agent (UA), the T-ball logo on the bottom right portion of the screen turns red since the "NtrtScan.exe" program keeps reloading.

Solution

This hot fix configures the "Agent Connection" setting to a global setting such that when it is changed, the Setting Aggregation File (SAF) package will be updated accordingly. This update enables the OfficeScan agents (managed by the Update Agent) to send a report to the OfficeScan server and instruct it to clear the configuration flag since there is a new setting.

Hot Fix Build 6258 (SBM 354263)

Issue

The OfficeScan server database may crash if the database backup path follows the universal naming convention (UNC) and the backup username length exceeds 32 characters.

Solution

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

Hot Fix Build 6258 (SBM 357331)

Issue

After administrators remove or uninstall the OfficeScan agent, the OfficeScan server removes all the OfficeScan agents from the database. This situation occurs when administrators set an agent unique identifier (UID) as a root domain UID.

Solution

This hot fix updates the OfficeScan server files to add two check points to resolve this issue.

Hot Fix Build 6258 (SBM 356698)

Enhancement

This hot fix provides a way for users to approve programs to run without checks by Meerkat (a detection improvement program that monitors newly encountered programs downloaded through HTTP or email applications).

Procedure

To approve programs to run without checking by Meerkat:

a. Install this hot fix (see "Installation").
b. Open the "Ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan server installation directory.
c. Under the "Global Setting" section, manually add the "MKWL" key and assign the encrypted string of the full program path.

[Global Setting]

MKWL = "The encrypted string of the full program path"

NOTE The encrypted string of the full program path needs to be provided by OfficeScan SEG engineer.

d. Save the changes and close the file.

e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.

f. Click "Save" to deploy the setting to agents.

The OfficeScan server deploys the command to OfficeScan agents and adds the following registry entry on all OfficeScan agent computers:

For x64 platform

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

For x86 platform

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

Key: MKWL

Type: String

Value: "The encrypted string of the full program path"

Hot Fix Build 6263/6300 (SBM 357949)

Issue

Automatic agent grouping uses rules defined by Microsoft™ Windows™ Active Directory (AD) domains. Sometimes, after the OfficeScan server synchronizes AD information from the Windows server, the status of enabled grouping rules shows a "Warning" sign.

Solution

This hot fix updates the OfficeScan programs to ensure that the enabled grouping rules will not be effected by the synchronized AD information.

Hot Fix Build 6263/6300 (SBM 357915)

Issue

While using the "Export Scan Exclusions" button, the "Scan Exclusion List (File Extensions)" function generates a "N/A" message in the exported CSV file when the "Scan Exclusion List (Files)" value is empty. This issue only happens in the "Scan Now" configuration.

Solution

This hot fix updates the OfficeScan programs to resolve this issue so that users can generate correct information in the CSV file.

Hot Fix Build 6263/6300 (SBM 357769)

Issue

OfficeScan leaks encrypted account passwords during web console operations. Unauthorized users could use the leaked encrypted password to log on to the OfficeScan server console.

Solution

This hot fix updates the OfficeScan server program to ensure that OfficeScan does not leak encrypted passwords.

Hot Fix Build 6263/6300 (SBM 358146)

Issue

If user set the default browser to Chrome™ and click on hyperlinks from other applications, the Chrome page shows a "try to access to an unexpected site "--disable-quic"" message.

Solution

This hot fix ensures that the Chrome page will not access unexpected "--disable-quic" sites when users click hyperlinks from other applications once they set Chrome™ as the default browser.

Hot Fix Build 6263/6300 (SBM 356873)

Enhancement

This hot fix enables users to generate the Secure Sockets Layer (SSL) certificate with SHA256 signature algorithm and 2048-bit public key for the OfficeScan web site which is installed on Microsoft™ Internet information Services (IIS) or Apache™ HTTP Server through the "SvrSvcSetup.exe" tool.

Procedure

To generate the SSL certificate with SHA256 signature algorithm and 2048-bit public key for manually renew the IIS SSL certificate:

a. Install this hot fix (see "Installation").
b. Log on as administrator, open a command prompt, and navigate to the "\PCCSRV\" directory.
c. Run the following command:

    SvrSvcSetup.exe –GenIISCert

d. A new SSL certificate is generated and is automatically added to the IIS SSL certificate store.
e. Open the IIS Manager console (inetmgr.exe).
f. Right-click the OfficeScan web site, and then click "Edit Bindings...".
g. When the "Site Bindings" window opens, select "https type" and click "Edit...".
h. Select the newly-created SSL certificate and click "OK".

    Note: Click the "View..." option to view the 2048-bit public key.

i. Click "Close".

To generate the SSL certificate with SHA256 signature algorithm and 2048-bit public key for manually renew the Apache™ SSL certificate:

a. Install this hot fix (see "Installation").
b. Log on as administrator, open a command prompt, and navigate to the "\PCCSRV\" directory.
c. Run the following command:

    SvrSvcSetup.exe –GenApacheCert

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

d. Stop the following services:
   OfficeScan Master Service
   Apache Service
e. Start the following services:
   Apache Service
   OfficeScan Master Service

Hot Fix Build 6267 (SBM 358436)

Issue

OfficeScan can synchronize suspicious objects and retrieve actions against these objects from a Control Manager server. However, an expired suspicious object is still synchronized to OfficeScan that makes false detections on the agent.

Solution

This hot fix updates the OfficeScan programs to ensure that the expired suspicious objects will not be detected.

Hot Fix Build 6267 (SBM 357701)

Issue

The "Agent Management" page of the OfficeScan web console may not display all OfficeScan agents if the domain has a large number of OfficeScan agents.

Solution

This hot fix resolves the issue by updating the mechanism used by the SQL table containing the OfficeScan agent information.

Hot Fix Build 6267 (SBM 354253)

Issue

The OfficeScan 11.0 Service Pack 1 Behavior Monitoring feature may block valid programs without leaving a record of the block action in the detection log.

Solution

This hot fix updates the OfficeScan Behavior Monitoring program to ensure that it blocks the correct programs.

Hot Fix Build 6271 (SBM 354682)

Issue

On x86 platforms, the Aegis module sends Meerkat detection information to the Officescan server and displays a pop-up dialog box that allows users to click on the "Allow Once" button. However, even afte users clicked on this button, Meerkat still blocks the application.

Solution

This hot fix updates Meerkat to check the payload of API events to prevent this issue from happening.

Hot Fix Build 6271 (SBM 356152)

Issue

The OfficeScan User-Mode Hooking (UMH) function prevents the "java.exe" program from working properly.

Solution

This hot fix adds "java.exe" onto the OfficeScan UMH whitelist pattern to ensure that the "java.exe" program works properly.

Hot Fix Build 6271 (SBM 357370)

Issue

The OfficeScan UMH function prevents the WebISO software from working properly.

Solution

This hot fix adds the WebISO software into the OfficeScan UMH whitelist pattern to ensure that the WebISO software works properly.

Hot Fix Build 6271 (SBM 358458)

Issue

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

Solution

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

Procedure

To configure OfficeScan to automatically block access to web sites that the TMUFE cannot rate:

a. Install this hot fix (see "Installation").

b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan server installation directory using a text editor.

c. Under the "Global Setting" section, manually add the following key and set its value to "1".

   [Global Setting]

   URLFilterErrMode = 1

d. Save the changes and close the file.

e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.

f. Click "Save" to deploy the setting to agents.

   The OfficeScan server deploys the command to OfficeScan agents and adds the following registry entry on all OfficeScan agent computers:

   Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC\TmProxy\Scan\Common\URLFilter\config

   Key: ErrMode

   Type: dword

   Value: 1

g. For Microsoft™ Windows™ 7/8/10 and Windows Server 2008 R2/2012/2016:

   Path:

   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey\Scan\Common\URLFilter\config

Key: ErrMode

Type: dword

Value: 1

h. Restart the OfficeScan agents.

Hot Fix Build 6274 (SBM 358714)

Issue

On the "Agents > Agent Management" section of the OfficeScan web console, when users run an advanced search for OfficeScan agents running with Update Agent "Disabled" status, the search results always display both OfficeScan agents running with Update Agent "Enabled" status and "Disabled" status.

Solution

This hot fix updates the OfficeScan server program to ensure that when users run an advanced search for OfficeScan agents running with Update Agent "Disabled" status, it displays the correct result.

Hot Fix Build 6274 (SBM 359007)

Issue

OfficeScan agents report their antivirus status information to the Microsoft™ Windows™ Security Center (WSC) when the system starts. However, after the system restarts, WSC displays that the OfficeScan antivirus reports are turned off.

Solution

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

Hot Fix Build 6274 (SBM 358753)

Issue

The OfficeScan NT Listener service ("TmListen.exe") may stop unexpectedly after the OfficeScan agent encounters a mismatch certificate error. When this happens, the agent update is unsuccessful.

Solution

This hot fix updates the OfficeScan agent program to prevent the "TmListen.exe" from stopping unexpectedly and ensures that the OfficeScan agent can handle the mismatch certificate error properly.

Hot Fix Build 6274 (SBM 358095)

Issue

DLP does not block the drag-and-drop of files from current Webmail sites (such as "Outlook.office.com" or "Outlook.live.com) when users use Google™ Chrome™ to access these Webmail sites.

Solution

This hot fix ensures that OfficeScan does not leak sensitive information when users use Google™ Chrome™ to access these Webmail sites.

Hot Fix Build 6277 (SBM 354730)

Enhancement

This hot fix enhances the OfficeScan server to support Active Directory subgroups for OfficeScan user accounts.

Procedure

To enable the new service settings:

a. Install this hot fix (see "Installation").
b. Open the "ofcserver.ini" file in the "\PCCSRV\Private" folder on the OfficeScan installation directory.
c. Under the "INI_AD_INTEGRATION_SECTION" section, manually add the following key and set its value to "1".

    [INI_AD_INTEGRATION_SECTION]

    RBAMultilayerInheritanceForADUser = 1
d. Save the changes and close the file.

Hot Fix Build 6281.1 (SBM 357771)

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.

Critical Patch 6285 (SBM 359321)

Issue

After installing OfficeScan Service Pack (SP1) Patch 1, the OfficeScan Smart Scan Pattern cannot be updated.

Solution

This critical patch updates the ActiveUpdate module to resolve the issue.

Hot Fix Build 6292 (SBM 358489)

Issue

OfficeScan Behavior Monitoring feature is unable to get the device type correctly when users launch programs by running as administrators (using administrator privileges).

Solution

This hot fix updates the Behavior Monitoring Service module to resolve this issue.

Hot Fix Build 6292 (SBM 359534)

Issue

An initialized issue related to the OfficeScan Control Manager Agent service ("OfcCMAgent.exe") may cause the OfcCMAgent.exe to stop unexpectedly.

Solution

This hot fix updates the OfficeScan Control Manager Agent program to prevent from this issue.

Hot Fix Build 6292 (SBM 360032)

Enhancement

This hot fix enables the Data Loss Prevention™ (DLP) Endpoint SDK 6.0 module starts to support the following Google™ Chrome™ versions:

- Google™ Chrome™ 55.0.2883.87
- Google™ Chrome™ 56.0.2924.87

Hot Fix Build 6292 (SBM 357707)

Enhancement

This hot fix enables the Address Space Layout Randomization (ASLR) of Data Loss Prevention™ (DLP) Endpoint SDK 6.0 for preventing DLL injection.

Hot Fix Build 6299 (SBM 357853)

Issue

When the "Protect documents against unauthorized encryption or modification" feature of Ransomware Protection is enabled, the OfficeScan agent may prevent a valid program from running if the size of the program file is too large.

Solution

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

Hot Fix Build 6299 (SBM 360097)

Issue

The Server Tuner tool optimizes the performance of the OfficeScan server. However, its Maximum Client Connections setting does not work.

Solution

This hot fix updates the OfficeScan server program to ensure that the tool's Maximum Client Connections setting works normally.

Hot Fix Build 6299 (SBM 357054)

Issue

When there are hot fix updates, the OfficeScan server checks all client components and prompts all clients with old hot fix versions to apply the updates including those where the No Program Upgrade option is enabled. This triggers a large number of unnecessary client notifications.

Solution

This hot fix ensures that the OfficeScan server does not notify a client of hot fix updates if the No Program Upgrade option is enabled in the client.

Hot Fix Build 6299 (SBM 359331)

Issue

The OfficeScan Behavior Monitoring program ("TMBMSRV.exe") crashes when the "MeerkatSkipUNC" option is enabled.

Solution

This hot fix updates the OfficeScan Behavior Monitoring program to correct this issue.

Hot Fix Build 6299 (SBM 359522)

Issue

When OfficeScan parses the contents of a policy that it receives from Control Manager™, some space characters may be removed from the policy which changes certain settings when applied to OfficeScan.

Solution

This hot fix ensures that OfficeScan can parse and apply Control Manager policies properly.

Hot Fix Build 6302 (JIRA 1587)

Issue

The "Quarantine malware variants detected in memory" feature needs to be enabled before the Memory Inspection Pattern (MIP) can be updated on OfficeScan agents.

Solution

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

Hot Fix Build 6302 (JIRA 1781)

Issue

Sometimes, the value of the "SourceUUID" setting in the "Ofcserver.ini" file is overwritten which prevents OfficeScan from updating the suspicious object list.

Solution

This hot fix ensures that the "SourceUUID" setting is not overwritten unexpectedly.

Hot Fix Build 6302 (JIRA 2639)

Issue

Sometimes, OfficeScan does not create system dump files when an exception error occurs.

Solution

This hot fix ensures that OfficeScan catches exception system codes and creates the corresponding system dump files when it encounters these codes.

Hot Fix Build 6306 (SBM 359200)

Issue

The "TMBMSRV.exe" process stops responding when debug log is enabled.

Solution

This hot fix resolves the issue by ensuring that the debug log output function receives the correct information.

Hot Fix Build 6306 (JIRA 2785)

Issue

Blue screen of death (BSOD) occurs when the OfficeScan agent AEGIS module runs simultaneously with an encryption software.

Solution

This hot fix enables the AEGIS module of OfficeScan agents to work normally with encryption software.

Hot Fix Build 6308 (JIRA 1474)

Issue

The Agent Connectivity widget displays inaccurate total number of connected clients for each Smart Protection Server information.

Solution

This hot fix updates the OfficeScan server program to ensure that the Agent Connectivity widget displays accurate information.

Hot Fix Build 6313 (JIRA 2354)

Issue

When users set the firewall exception rule to a single IP, the IP address does not appear on the OfficeScan agent console.

Solution

This hot fix ensures that the IP address appears on the OfficeScan agent console.

Hot Fix Build 6313 (JIRA 3487)

Issue

It takes a long time to export the scan exclusion list from the OfficeScan web console.

Solution

This hot fix improves the export function to enable OfficeScan to export the scan exclusion list faster.

Hot Fix Build 6313 (JIRA 1442)

Issue

A Microsoft™ Windows™ Security audit failure by "tmevtmgr.sys" appears in the Windows system event log.

Solution

This hot fix resolves the issue by enabling the build option in the AEGIS driver to include a "path hash".

Hot Fix Build 6313 (JIRA 3616)

Issue

When an OfficeScan agent downloads a file that does not have a valid digital signature, the file path information in the corresponding system event log will be truncated on the OfficeScan web console.

Solution

This hot fix ensures that system event logs display the complete file path information on the OfficeScan web console.

Hot Fix Build 6315/6331 (SBM 350467/JIRA 4506)

Enhancement

This hot fix enables the Behavior Monitoring approved list to support the asterisk (*) and question mark (?) wildcard characters in program path names and file names.

Hot Fix Build 6317 (JIRA 2809/JIRA 3533/JIRA 3668)

Issue

Blue screen of death (BSOD) occurs when the OfficeScan agent AEGIS module runs simultaneously with an encryption software.

Solution

This hot fix enables the AEGIS module of OfficeScan agents to work normally with encryption software.

Critical Patch 6325 (VRTS-283)

Issue

When the Web Reputation Service (WRS) of the OfficeScan agent program blocks access to a certain webpage, it displays the "Website blocked by Trend Micro OfficeScan" alert page instead. This alert page may be affected by XSS vulnerabilities.

Solution

This critical patch updates the OfficeScan agent program to resolve the XSS vulnerabilities.

Critical Patch 6325 (VRTS-393/SBM 357769)

Issue

Encrypted account passwords may leak out during web console operations. Unauthorized users could use the leaked encrypted password to log on to the OfficeScan server console.

Solution

This critical patch ensures that encrypted passwords are secure during web console operations.

Critical Patch 6325 (VRTS-615)

Enhancement

This critical patch updates the OfficeScan agent program to improve its self-protection mechanism to protect against a local attacker to inject malicious code.

Hot Fix Build 6325 (JIRA 1715)

Issue

It takes a long time for the Windows™ Disk Manager to start when OfficeScan's Ravage Scan feature is enabled.

Solution

This hot fix enables users to configure the OfficeScan Ravage Scan feature to skip a specific virtual hard disk to allow the Disk Manager to start normally.

Procedure

To enable the Ravage Scan feature to skip a specific virtual hard disk:

a. Install this hot fix (see "Installation").
b. Open the Registry Editor.
c. Add the following key:

Path:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\tmactmon\Parameters]

Type: dword

Key: SkipVirtualHarddisk

Data Value: 00000001

d. Restart the OfficeScan client computer.

Hot Fix Build 6325 (JIRA 2673)

Issue

PccNT.exe stops unexpectedly because the following agent registry contains a value that is larger than the maximum supported value.

Path:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\

\Misc.]

Type: dword:7fffffff

Key: TotalScanned

Solution

This hot fix updates the "fcWofieUI.dll" (for 32-bit) and "fcWofieUI_64x.dll" (for 64-bit) OfficeScan agent files to solve this issue.

Hot Fix Build 6325 (SBM 359608)

Issue

Users cannot run a manual sync on the "Suspicious Object List Setting" page when the "Enable Suspicious URL list" option is disabled.

Solution

This hot fix ensures that manual sync can complete successfully when the "Enable Suspicious URL list" option is disabled.

Hot Fix Build 6325 (JIRA 3289)

Issue

The error-handling mechanism of POP3 and SMTP scans may attempt to access tmp files which can trigger the TmListen service to stop unexpectedly.

Solution

This hot fix resolves the issue by ensuring that the error-handling mechanism accesses only valid local file paths.

Hot Fix Build 6325.1 (JIRA 2812)

Issue

Garbled characters appear in POP3 email notification for malicious email message contents.

Solution

This hot fix resolves the issue by changing the text encoding format for POP3 email notifications from West Europe to shift-JIS.

Hot Fix Build 6331 (SBM 358992)

Issue

Users cannot access the "Advanced Search" web page from the "Firewall Profile Settings" page of the OfficeScan web console.

Solution

This hot fix updates the OfficeScan server program files to ensure that users can access the "Advanced Search" web page from the "Firewall Profile Settings" page.

Hot Fix Build 6331 (JIRA 1891)

Issue

The DLP module may not work normally while other programs are uploading files to the Internet.

Solution

This hot fix ensures that the DLP module works normally when other programs are to uploading files to the Internet.

Hot Fix Build 6331 (JIRA 4537)

Issue

Blue screen of death (BSOD) occurs when the OfficeScan agent AEGIS module runs simultaneously with an encryption software.

Solution

This hot fix enables the AEGIS module of OfficeScan agents to work normally with encryption software.

Issues resolved by hot fixes for OfficeScan XG

Hot Fix B1253	Hot Fix B1254	Hot Fix B1255	Hot Fix B1262	Hot Fix B1265	Hot Fix B1265.1	Hot Fix B1269	Hot Fix B1270
Hot Fix B1270.1	Hot Fix B1277	Hot Fix B1289	Hot Fix B1292	Hot Fix B1293	Hot Fix B1308	Hot Fix B1314	CP1315
Hot Fix B1318	Hot Fix B1320	Hot Fix B1321	Hot Fix B1322	Hot Fix B1325	Hot Fix B1331	Hot Fix B1334	Hot Fix B1340
Hot Fix B1341	Hot Fix B1343	Hot Fix B1346	Hot Fix B1347	Hot Fix B1349	CP1352 / 1429	Hot Fix B1412	Hot Fix B1415
Hot Fix B1417	Hot Fix B1420	Hot Fix B1422	Hot Fix B1423				

Hot Fix Build 1253 (SBM 355172)

Issue

The DLP module cannot block users from sending out email messages with illegal file attachments through Webmail.

Solution

This hot fix updates the HTTPS parser to ensure that the DLP module can block users from sending out email messages with illegal file attachments through Webmail.

Hot Fix Build 1254 (SBM 355446)

Issue

The "Unmanaged Endpoints" page of the OfficeScan web console may not display the progress of the agent installation task if a selected endpoint under the Active Directory (AD) contains an ampersand character "&".

Solution

This hot fix ensures that the "Unmanaged Endpoints" page displays the progress of the agent installation task.

Hot Fix Build 1255 (SBM 355573)

Issue

The "Update Agent" drop down list in the "Add IP Range and Update Source" page displays only one Update Agent even when multiple Update Agents are available. As a result, users cannot select any other Update Agent.

Solution

This hot fix updates the OfficeScan server files to ensure that the "Update Agent" drop down list displays all available Update Agents.

Hot Fix Build 1262 (SBM 356409)

Issue

When the OfficeScan server receives a policy from a Control Manager 6.0 server and the policy contains space characters, OfficeScan will not be able to apply the policy effectively.

Solution

This hot fix updates the OfficeScan server files to ensure that the OfficeScan server can parse space characters in policies correctly and implement these policies successfully.

Hot Fix Build 1265 (SBM 356681)

Issue

The OfficeScan server console returns gateway errors when trying to export the agent list using the following views:

- Anti-spyware View
- Data Protection View
- Firewall View

Solution

This hot fix updates the export function to properly retrieve the complete agent list inventory for all views.

Hot Fix Build 1265 (SBM 356463)

Issue

The OfficeScan Master Service suffers a crash after attempting to reuse freed memory.

Solution

This hot fix ensures that the OfficeScan Master Service release the memory after no other procedures are referencing.

Hot Fix Build 1265.1 (SBM 356615/SBM 356820)

Enhancement

This hot fix updates the Data Loss Prevention™ Endpoint SDK 6.2 to support Google™ Chrome™ version 54.0.2840.99.

Hot Fix Build 1269 (SBM 356494/SBM 357105)

Enhancement

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features.

This hot fix updates OfficeScan agent programs and the Contextual Intelligence Engine ("tmxfalcon.dll") to provide more accurate and efficient functions in Trend Micro Predictive Machine Learning.

Hot Fix Build 1270 (SBM 356668)

Issue

The OfficeScan XG Behavior Monitoring feature blocks a valid program.

Solution

This hot fix updates the OfficeScan Behavior Monitoring Local Pattern to ensure that it blocks the correct programs.

Hot Fix Build 1270.1 (SBM 354880)

Issue

OfficeScan's DLP blocks the following software applications:

- Skype™ for Business Cloud Storage Channel
- Office Telemetry

Solution

This hot fix updates the OfficeScan's iDLP module to resolve this issue.

Hot Fix Build 1277 (SBM 354880)

Issue

Trend Micro Data Loss Prevention™ (DLP) module blocks Skype™ for Business unexpectedly and caused a false alert on Cloud Storage channel.

Solution

This hot fix updates the HTTPS parser to ensure that the DLP module does not block communication of Skype™ for Business.

Hot Fix Build 1277 (SBM 357326)

Issue

The DLP cannot block the violative documents with a policy that only includes File Attribute.

Solution

This hot fix updates the matching result to ensure that the DLP module can block violative documents.

Hot Fix Build 1277 (SBM 357706/SBM 356820/SBM 357553)

Enhancement

This hot fix enables Data Loss Prevention™ Endpoint SDK 6.2 starts to support Google™ Chrome™ version 55.0.2883.75.

Hot Fix Build 1289 (SBM 357043)

Issue

After users upgrade OfficeScan agents to OfficeScan XG on a computer running on the 32-bit version of Microsoft™ Windows™, OfficeScan agents may keep restarting hourly.

Solution

This hot fix resolves this issue by updating the OfficeScan server program to ensure that OfficeScan agents upgrade to OfficeScan XG properly.

Hot Fix Build 1289 (SBM 358146)

Issue

If user set the default browser to Chrome™ and click on hyperlinks from other applications, the Chrome page shows a "try to access to an unexpected site "--disable-quic"" message.

Solution

This hot fix ensures that the Chrome page will not access unexpected "--disable-quic" sites when users click hyperlinks from other applications once they set Chrome™ as the default browser.

Hot Fix Build 1289 (SBM 357664)

Issue

In Microsoft™ Windows™ Vista/2008 or later clients, OfficeScan displays an incorrect firewall driver version number. The correct version number is 5.83.1003, but the version number that OfficeScan displays is 5.82.1089.

Solution

This hot fix ensures that the OfficeScan server references the "tmlwf.sys" and "tmwfp.sys" files to determine the correct version number of the common firewall driver

Hot Fix Build 1289 (SBM 356522)

Enhancement

This hot fix enhances the sample submission process from the OfficeScan server to the Deep Discovery Analyzer (DDAN) server through a proxy server. This hot fix also enhances the error handling functions for sample submission analysis.

To configure for the proxy, please refer to following:

New keys:

UseProxy = 1

ProxyServer = xxx.xxx.xxx.xxx

ProxyPort = xxxx

ProxyLogin = xxxx

ProxyPwd = xxxx

Add the new keys to the "Sample_Submission" section of of the cDdaSvr.ini file as follows:

[Sample_Submission]

OfcDdaServerRegistered = 1

Server = xxx.xxx.xxx.xxx

APIKey = xxxxxxxx

UseProxy = 1

ProxyServer = xxx.xxx.xxx.xxx

ProxyPort = xxxx

ProxyLogin = xxxxx

ProxyPwd = xxxxx

Hot Fix Build 1292 (SBM 354631)

Enhancement

This hot fix adds a way to configure OfficeScan clients to skip digital signature checking of OfficeScan client program files while downloading hot fix files and reloading the scan engine.

Procedure

To prevent OfficeScan clients from checking the digital signature of program files while downloading hot fix files and reloading the scan engine:

a. Install this hot fix (see "Installation").

b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder of the OfficeScan installation directory.

c. Under the "Global Setting" section, add the following key and set its value to "1".

[Global Setting]

DOVF = 1

j. Save the changes and close the file.

k. Open the OfficeScan server management console and go to "Agents > Global Agent Settings".

l. Click "Save" to deploy the setting to all clients.

m. Restart the OfficeScan client.

e. The OfficeScan client program automatically installs the following registry key:

Path:

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

Key: DOVF

Value: 1

Hot Fix Build 1293 (SBM 358410/SBM 358027)

Issue

The TmListen.exe service of the OfficeScan agent stops unexpectedly after the OfficeScan agent encounters a certificate mismatch.

Solution

This hot fix enhances error-handling mechanism on the OfficeScan agent to prevent TmListen.exe from stopping unexpectedly until the agent can handle the certificate mismatch event.

Hot Fix Build 1308 (SBM 352397)

Issue

The "Last Spyware Detection(Real-time)" agent information column name shows as "Last Spyware Scan(Real-time)" in the exported CSV file.

Solution

This hot fix updates the program and modifies the "Last Spyware Scan(Real-time)" column name to "Last Spyware Detection(Real-time)" in the CSV file.

Hot Fix Build 1308 (SBM 358345)

Issue

SQL exceptions somehow continue to occur in the system event log and causes Internet Information Services (IIS) to crash.

Solution

This hot fix updates the OfficeScan server files to ensure that the OfficeScan server and IIS server works properly.

Hot Fix Build 1308 (SBM 358044)

Issue

The Microsoft™ Windows™ Event Log generates too many messages.

Solution

This hot fix enables OfficeScan to extend the cache time to 12 hours.

Hot Fix Build 1308 (SBM 358404)

Issue

On some OfficeScan agents managed by the Update Agent (UA), the OfficeScan agent icon on the Microsoft™ Windows™ task bar may be shaded red and blue repeatedly and shows a "Protection at Risk" message. This issue occurs since the Real-time Scan service is not functional.

Solution

This hot fix updates the OfficeScan server and agent programs to ensure that the OfficeScan agents managed by the Update Agent can work normally without errors.

Hot Fix Build 1308 (SBM 358940)

Issue

Compatibility issues occur between the third-party OpenSSL libraries used in the new types of processors (for example, the Apollo Lake Intel™ Pentium(R) processor).

Solution

This hot fix replaces the OfficeScan server files to resolve this issue.

Hot Fix Build 1308 (SBM 358516)

Issue

A performance enhancement introduced a negative side effect that causes a memory leak on "NTRtScan.exe".

Solution

This hot fix disables the performance enhancement to resolve this issue.

Hot Fix Build 1308 (SBM 358095)

Issue

DLP does not block the drag-and-drop of files from current Webmail sites (such as "Outlook.office.com" or "Outlook.live.com) when users use Google™ Chrome™ to access these Webmail sites.

Solution

This hot fix ensures that OfficeScan does not leak sensitive information when users use Google™ Chrome™ to access these Webmail sites.

Hot Fix Build 1308 (SBM 357444)

Enhancements

This hot fix enables users to generate the Secure Sockets Layer (SSL) certificate with SHA-256 signature algorithm and 2048-bit public key for the OfficeScan web site, which is installed on Microsoft Internet Information Services (IIS) through the "SvrSvcSetup.exe" tool.

Procedure

To generate the SSL certificate with SHA-256 signature algorithm and 2048-bit public key, and manually renew the IIS SSL certificate:

d. Log on as administrator, open a command prompt, and navigate to the "\PCCSRV\" directory.

e. Run the following command:

SvrSvcSetup.exe –GenIISCert

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

n. Open the IIS Manager console (inetmgr.exe).

o. Right-click the OfficeScan web site, and then click "Edit Bindings...".

p. When the "Site Bindings" window opens, select "https type" and click "Edit...".

q. Select the newly-created SSL certificate and click "OK".

Note: Click the "View..." option to view the SHA256 signature algorithm and 2048-bit public key.

r. Click "Close".

Hot Fix Build 1314 (SBM 357421)

Issue

The OfficeScan NT Real-time Scan service ("Ntrtscan.exe") may stop unexpectedly on endpoints running Microsoft™ Windows™ Embedded 7.

Solution

This hot fix updates the OfficeScan agent program to resolve this issue on affected endpoints.

Hot Fix Build 1314 (SBM 358192)

Issue

The "Unmanaged Endpoints of Schedule Assessment" report displays many OfficeScan agents as "Managed by another OfficeScan server" even though the endpoints are managed by the OfficeScan server.

Solution

This hot fix resolves the issue by changing the checking mechanism on the OfficeScan server to be case insensitive.

Hot Fix Build 1314 (SBM 359293)

Issue

The virus outbreak notifications only display a single entry.

Solution

This hot fix replaces the OfficeScan server files to resolve this issue.

Critical Patch 1315 (SBM 356677)

Issue

In OfficeScan XG, users may observe that "OfcService.exe" crashes and OfficeScan agents keep updating in some situations.

Solution

This critical patch replaces the OfficeScan server files to resolve the issue.

Critical Patch 1315 (SBM 360001/SBM 360132)

Issue

The OfficeScan XG server program and the OfficeScan agent Smart Scan common module uses an OpenSSL version that is affected by certain vulnerabilities.

Solution

This critical patch resolves this issue by updating the OpenSSL component of the server module and Smart Scan common module.

Hot Fix Build 1318 (SBM 359826)

Issue

The OfficeScan XG Behavior Monitoring feature blocks a valid program.

Solution

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

Hot Fix Build 1320 (SBM 360060)

Issue

The TmListen.exe service of the OfficeScan agent stops unexpectedly when Web Reputation Service is running.

Solution

This hot fix updates the OfficeScan agent programs to prevent TmListen.exe from stopping unexpectedly.

Hot Fix Build 1321 (JIR-1194)

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 XG server and agent files to ensure that agents can still trigger scheduled updates when these agents cannot connect to OfficeScan server during startup.

Hot Fix Build 1321 (SBM 359260)

Issue

The OfficeScan NT Real-time Scan service may cause the Microsoft™ Windows™ system to hang.

Solution

This hot fix updates the Behavior Monitoring Core Service programs of the OfficeScan agent to resolve this issue.

Hot Fix Build 1321 (SBM 359630)

Issue

Microsoft™ Outlook™ takes some time to load whenever DLP is enabled.

Solution

This hot fix resolves the issue wherein Microsoft™ Outlook™ takes too long to launch by updating the "sakfile.sys" file of DLP by adding "Outlook.exe" onto the exception list.

Hot Fix Build 1321 (SBM 358898/SBM 360065)

Enhancement

This hot fix enables Data Loss Prevention™ Endpoint SDK 6.0 starts to support the following Google™ Chrome™ versions:

- Google™ Chrome™ 55.0.2883.87
- Google™ Chrome™ 56.0.2924.87

Hot Fix Build 1321 (SBM 359660)

Enhancement

This hot fix enables Data Loss Prevention™ Endpoint SDK 6.2 to support Microsoft™ OneNote 2016 with *.one file type.

Hot Fix Build 1322 (SBM 359535)

Issue

An initialized issue related to the OfficeScan Control Manager Agent service ("OfcCMAgent.exe") may cause the OfcCMAgent.exe to stop unexpectedly.

Solution

This hot fix updates the OfficeScan Control Manager Agent program to prevent from this issue.

Hot Fix Build 1322 (SBM 359636)

Issue

When users export the settings from a root domain to a subdomain, the subdomain does not inherit the sample submission settings.

Solution

This hot fix ensures that the OfficeScan server sets the flag to "ofcscan.ini" when exporting settings so that the subdomain inherits all the settings from the root domain.

Hot Fix Build 1322 (SBM 359257)

Issue

Microsoft™ Skype™ for Business hangs when the OfficeScan agent is running.

Solution

This hot fix updates the OfficeScan agent module files inside the Common Client Solution Framework (CCSF) to prevent third-party software from hanging.

Hot Fix Build 1325 (SBM 356626)

Enhancement

This hot fix updates the OfficeScan Data Loss Prevention™ (DLP) module to enable its Device Control feature to work on portable devices with read-only permission.

Procedure

To enable the new service settings:

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan installation directory.
c. Under the "Global Setting" section, manually add the following key and set its value to "1".

    [Global Setting]

    InstallDLPWpdDriver = 1

d. Save the changes and close the file.

e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.

f. Click "Save" to deploy the setting to clients.

Path:

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\DlpLite

Key: InstallDLPWpdDriver

Type: DWORD

Value:

0 = Device Control does not work on portable devices with read-only permission

1 = Device Control works on portable devices with read-only permission

Hot Fix Build 1331 (JIRA 1927)

Issue

OfficeScan leaks encrypted account passwords during web console operations. Unauthorized users could use the leaked encrypted password to log on to the OfficeScan server console.

Solution

This hot fix ensures that OfficeScan does not leak encrypted passwords.

Hot Fix Build 1331 (SBM 359497)

Issue

Certain processes running on the email channel may trigger policies in other channels.

Solution

This hot fix updates OfficeScan's rule matching method to ensure that processes will trigger only the policies for the current channel.

Hot Fix Build 1331 (JIRA 1362/JIRA 1365)

Issue

The Integrated Smart Protection Server and the standalone Smart Protection Server cannot parse the information in the "User Agent" header because it is in the wrong format.

Solution

This hot fix ensures that the iCRC common module adds information into the "User Agent" header in the correct format.

Hot Fix Build 1334 (JIRA 2329)

Issue

The OfficeScan agent installs an unnecessary certificate "ofcsslagent" on the agent computer.

Solution

This hot fix removes the "ofcsslagent" certificate and ensures that the OfficeScan agent no longer installs this to agent computers.

Hot Fix Build 1334 (JIRA 2473)

Issue

The OfficeScan NT Firewall service still appears on the Windows™ Action Center console after the OfficeScan agent is uninstalled from the computer.

Solution

This hot fix updates the OfficeScan agent programs to successfully unregister its Firewall service from the Windows™ Action Center console.

Hot Fix Build 1334 (JIRA 2160)

Issue

The maximum size for a single file to upload is 5 MB but the OfficeScan client still attempts to upload files that are larger than 5 MB to the server. This causes heavy traffic on the server.

Solution

This hot fix syncs the 5 MB limit to OfficeScan clients to ensure that the clients do not attempt to upload larger files to the OfficeScan server.

Hot Fix Build 1334 (JIRA 1175)

Enhancement

This hot fix allows users to disable the email multi-part scan mode in the DLP function of OfficeScan agents.

Procedure

To disable the email multi part scan mode in the DLP function and globally deploy this setting to all OfficeScan agents:

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder of the OfficeScan server.
c. Under the "Global Setting" section, manually add the following key and set its value to "0".

   [Global Setting]

   EnableDlpMPScan = 0

   NOTE To enable the setting again, set "EnableDlpMPScan=1".

d. Save the changes and close the file.
e. Open the OfficeScan server management console and click "Agents > Global Agent Settings" on the main menu to access the "Global Agent Settings" page.
f. Click "Save" to deploy the setting to agents.

The OfficeScan server deploys the command to agents and adds the following registry entry on all agent computers:

Path:
HKLM\SYSTEM\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\DlpLite
Key: EnableMPScan
Type: dword
Value: 0

Hot Fix Build 1340 (JIRA 2701)

Issue

Users cannot remove items from the "Favorites" menu on the OfficeScan web console.

Solution

This hot fix updates the OfficeScan files to enable users to delete items from the "Favorites" menu.

Hot Fix Build 1340 (JIRA 1640)

Issue

The DLP version appears as 0.0.0 on both the management console and agent console.

Solution

This hot fix ensures that the correct DLP version appears on both the management console and agent console.

Hot Fix Build 1340 (JIRA 3355)

Issue

OfficeScan agents report their antivirus status information to the Microsoft™ Windows™ Security Center (WSC) when the system starts. However, after the system restarts, WSC displays that the OfficeScan antivirus reports are turned off.

Solution

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

Hot Fix Build 1340 (JIRA 1184)

Issue

Certain processes running on the email channel may trigger policies in other channels.

Solution

This hot fix updates OfficeScan's rule matching method to ensure that processes will trigger only the policies for the current channel.

Hot Fix Build 1340 (JIRA 3016)

Enhancement

This hot fix enables Data Loss Prevention™ Endpoint SDK 6.0 starts to support the following Google™ Chrome™ versions:

- Google™ Chrome™ 57.0.2987.98
- Google™ Chrome™ 57.0.2987.110

Hot Fix Build 1341 (JIRA 2319)

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 hot fix 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.

Procedure

To disable the self-protection feature of the AEGIS module in affected computers:

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder of the OfficeScan installation directory.
c. Under the "Global Setting" section, add the following key and set its value to "1".
   [Global Setting]
   SkipDuplicateSameAccess = 1
d. Save the changes and close the file.
e. Open the OfficeScan server management console and go to "Agents > Global Agent Settings".
f. Click "Save" to deploy the setting to all clients.
g. Restart the OfficeScan client.

The OfficeScan client program automatically installs the following registry key:

PATH:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tmactmon\Parameters
KEY: SkipDuplicateSameAccess
TYPE: dword
VALUE:
1, disables the self-protection feature
0, enables the self-protection feature

Hot Fix Build 1343 (JIRA 2354)

Issue

When users set the firewall exception rule to a single IP, the IP address does not appear on the OfficeScan agent console.

Solution

This hot fix ensures that the IP address appears on the OfficeScan agent console.

Hot Fix Build 1343 (JIRA 2420)

Issue

The suspicious object URL detection function does not work when the OfficeScan agent is offline.

Solution

This hot fix enables the suspicious object URL detection function to work when the OfficeScan agent is offline.

Hot Fix Build 1343 (JIRA 3372)

Issue

Sensitive information detected in email messages in "outlook.com" and "outlook.office.com" are displayed in the logs as HTTP channels and not as webmail channels.

Solution

This hot fix updates the DLP module to make sure OfficeScan assigns the correct channels in the logs.

Hot Fix Build 1343 (JIRA 3237)

Issue

An issue prevents OfficeScan agents from blocking webmail attachments that contain sensitive information in "outlook.com".

Solution

This hot fix updates the DLP module to make sure the OfficeScan agent can block webmail attachments in "outlook.com".

Hot Fix Build 1346 (JIRA 2594)

Issue

The OfficeScan Behavior Monitoring feature may cause certain operating systems to stop unexpectedly when users launch an Intel driver packed as a self-extracting RAR file.

Solution

This hot fix updates the Behavior Monitoring Service module to resolve the issue.

Hot Fix Build 1346 (JIRA 3749)

Issue

A configuration issue prevents the WRS from working.

Solution

This hot fix updates the OfficeScan WRS file to resolve the configuration issue and ensure that WRS works normally.

Hot Fix Build 1346 (JIRA 3160)

Issue

When users click the "Specify Domain Credentials" button on the OfficeScan XG web console, it caches the credentials of the Active Directory Integration account in plain text.

Solution

This hot fix updates the OfficeScan server program to prevent it from decrypting the Active Directory Integration account password to ensure that the password does not appear in plain text on the web console.

Hot Fix Build 1347 (JIRA 3734)

Issue

This issue occurs because the Web Reputation Services is disabled, OfficeScan agents still search for available Smart Protection Servers (SPS) to send Web Reputation queries to which can keep the network busy.

Solution

This hot fix adds an option to prevent OfficeScan agents from searching for Local Web Classification Servers (LWCS) when the WRS is disabled.

Procedure

To enable this option:

a. Install this hot fix (see "Installation").
b. Open the "Ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan installation directory.
c. Add the following key under the "ICRC_SCAN_INI_SECTION" section and set its value to "0".

    [ICRC_SCAN_INI_SECTION]
    WCSServiceSearchIfDisabled = 0

d. Open the OfficeScan web console and go to the "Networked Computers > Global Client Settings" screen.
e. Click "Save" to deploy the setting to clients.

The OfficeScan client program automatically installs the following registry key:

Path: HKLM\SOFTWARE\TrendMicro\Pc-cillinNTCorp\CurrentVersion\iURL Scan\
Key: ServiceSearchIfDisabled
Value: 0

Hot Fix Build 1349 (JIRA 4276)

Issue

OfficeScan agents keep on upgrading when the "PostponedInst" folder contains a file with a lower version even when the timestamp on the file is current.

Solution

This hot fix resolves the issue by adding more checking mechanisms on OfficeScan agents.

Hot Fix Build 1349 (JIRA 3093)

Issue

The integrated DLP API hook does not work on Windows™ 10 Red Stone 2 (RS2) RTM build (15063).

Solution

This hot fix resolves this issue.

Hot Fix Build 1349 (SBM 360059)

Issue

The FortiClient VPN program may encounter connection issues on computers protected by OfficeScan XG.

Solution

This hot fix resolves a compatibility issue between FortiClient VPN and the DLP module

Critical Patch 1352/Critical Patch 1429 (VRTS-283)

Issue

When the Web Reputation Service (WRS) of the OfficeScan agent program blocks access to a certain webpage, it displays the "Website blocked by Trend Micro OfficeScan" alert page instead. This alert page may be affected by XSS vulnerabilities.

Solution

This critical patch updates the OfficeScan agent program to resolve the XSS vulnerabilities.

Critical Patch 1352/Critical Patch 1429 (VRTS-393)

Issue

Encrypted account passwords may leak out during web console operations. Unauthorized users could use the leaked encrypted password to log on to the OfficeScan server console.

Solution

This critical patch ensures that encrypted passwords are secure during web console operations.

Critical Patch 1352/Critical Patch 1429 (VRTS-615)

Enhancement

This critical patch updates the OfficeScan agent program to improve its self-protection mechanism to protect against a local attacker to inject malicious code.

Hot Fix Build 1412 (JIRA 1362/JIRA 1365)

Issue

The Integrated Smart Protection Server and the standalone Smart Protection Server cannot parse the information in the "User Agent" header because it is in the wrong format.

Solution

This hot fix ensures that the iCRC common module adds information into the "User Agent" header in the correct format.

Hot Fix Build 1415 (JIRA 1678)

Enhancement

This hot fix updates the OfficeScan Data Loss Prevention™ (DLP) module to enable its Device Control feature to work on portable devices with read-only permission.

Procedure

To enable the new service settings:

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder on the OfficeScan installation directory.
c. Under the "Global Setting" section, manually add the following key and set its value to "1".

    [Global Setting]

    InstallDLPWpdDriver = 1
d. Save the changes and close the file.
e. Open the OfficeScan web console and go to the "Agents > Global Agent Settings" screen.
f. Click "Save" to deploy the setting to clients.

    Path:

    HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\DlpLite

    Key: InstallDLPWpdDriver

    Type: DWORD

Value:

0 = Device Control does not work on portable devices with read-only permission

1 = Device Control works on portable devices with read-only permission

Hot Fix Build 1417 (JIRA 2160)

Issue

The maximum size for a single file to upload is 5 MB but the OfficeScan client still attempts to upload files that are larger than 5 MB to the server. This causes heavy traffic on the server.

Solution

This hot fix syncs the 5 MB limit to OfficeScan clients to ensure that the clients do not attempt to upload larger files to the OfficeScan server.

Hot Fix Build 1420 (JIRA 2766)

Issue

The OfficeScan NT Real-time Scan service may cause the Microsoft™ Windows™ system to hang.

Solution

This hot fix updates the Behavior Monitoring Core Service programs of the OfficeScan agent to resolve this issue.

Hot Fix Build 1420 (JIRA 2701)

Issue

Users cannot remove items from the "Favorites" menu on the OfficeScan web console.

Solution

This hot fix updates the OfficeScan files to enable users to delete items from the "Favorites" menu.

Hot Fix Build 1422 (JIRA 2319)

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 hot fix enables users to disable the self-protection feature of the AEGIS module for AvayacScopia to prevent the incompatibility issue and ensure that Avaya Scopia can run normally on protected computers.

Procedure

To disable the self-protection feature of the AEGIS module in affected computers:

a. Install this hot fix (see "Installation").
b. Open the "ofcscan.ini" file in the "\PCCSRV\" folder of the OfficeScan installation directory.
c. Under the "Global Setting" section, add the following key and set its value to "1".

    [Global Setting]

    SkipDuplicateSameAccess = 1
d. Save the changes and close the file.
e. Open the OfficeScan server management console and go to "Agents > Global Agent Settings".
f. Click "Save" to deploy the setting to all clients.
g. Restart the OfficeScan client.

The OfficeScan client program automatically installs the following registry key:

PATH:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tmactmon\Parameters
KEY: SkipDuplicateSameAccess
TYPE: dword
VALUE:
1, disables the self-protection feature
0, enables the self-protection feature

Hot Fix Build 1423 (JIRA 3227/JIRA 3119)

Issue

OfficeScan agents report their antivirus status information to the Microsoft™ Windows™ Security Center (WSC) when the system starts. However, after the system restarts, WSC displays that the OfficeScan antivirus reports are turned off.

Solution

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