Trend Micro OfficeScan XG
Change Management Request Form

10th August 2018

OVERVIEW

This document is intended to make the customer's process of upgrading easier and minimize unnecessary time delays. The change management request process is really tedious as there are several items needed to be fulfilled before escalating it to the Change Approval Board (CAB). Members of the CAB evaluate change requests. The CAB members make recommendations that are based on the impact on existing services, the cost of the change, and other relevant factors.

OSCE XG SERVICE PACK 1

Change Summary

Summary Description	Upgrade OfficeScan XG to OfficeScan XG Service Pack 1 (SP1)
Change Reason	Upgrade
Change Type	Significant
Priority	High
Risk Level	Medium
Timing	Normal

Description

The repacked version (r1) of OfficeScan XG Service Pack 1 (SP1) is now available in the Trend Micro Download Center. It contains cumulative fixes and additional features.

What's New	Release Date	Size (MB)
• Enhanced "Fileless" Script Detections • Windows 10 Fall Creators Update (Version 1709) Support • Update Agent Connections • Behavior Monitoring wildcard characters exception List • Predictive Machine Learning • Cloud Synchronization Channel for Ransomware Detections • Proxy Settings Enhancement	2017-12-06	1000

• Suspicious Object Lists • OfficeScan Data Protection Enhancements - GDPR compliance and User-based Device Control		

Release Info

OSCE XG SP1	Build 4345 Download link
Product Documentation	Administrator's Guide link Server Readme link Agent Readme link System Requirement link
Hotfixes included in OSCE XG SP1	https://success.trendmicro.com/solution/111855
Network Traffic for Upgrading OfficeScan Agents	32-bit endpoint = 104 MB 64-bit endpoint = 142 MB
Requires Reboot after installation	☑ Yes (All Endpoints)

Implementation, Test and Backout Plan

Implementation Plan

Prerequisites:

- OfficeScan XG SP1 automatically upgrades the scan engine on the OfficeScan server and all OfficeScan agents immediately after installation (regardless of OfficeScan agent update settings).
- Trend Micro recommends performing the upgrade during off-peak hours to minimize network disruptions.
- Rebooting the OfficeScan server machine may be necessary if you are installing on Windows Server 2012 and the following components are updated:
  - Microsoft .NET Framework 4.6.1 Full
  - Microsoft SQL server 2012 Native Client
- After upgrading OfficeScan agents to OfficeScan XG SP1, you must restart the agent endpoints to ensure that the OfficeScan agent program properly adopts the HTTPS module and continues to properly communicate with the OfficeScan server.
- This service pack can only be used to upgrade OfficeScan XG. If you are using OfficeScan 11.0, please upgrade to OfficeScan XG first.

Installing OfficeScan XG SP1:

1. Download the package from Trend Micro Download Center.
2. Run the package.
3. Follow the installation procedure
4. Once installation finished, the services will be restarted.
5. Functional verification of test plan

Test Plan	Backout Plan
[OfficeScan Server] • Service pack installation completed without errors • OfficeScan console can be accessed without issue • Help > About of OfficeScan console shows "XG Service Pack 1" • OfficeScan settings are intact • All agents are showing in the console • All OfficeScan Server services are running [OfficeScan Agent] • All OfficeScan Client services are running • OfficeScan agent icon is present in the system tray without errors • Can launch OSCE agent console	• Create VM snapshot before upgrading OfficeScan • Backup OfficeScan Server and Database before upgrade • Restore OfficeScan Server and Database • Functional Verification of Backout plan

OSCE XG SP1 Critical Patch

Change Summary

Summary Description	Apply OfficeScan XG Critical Patch build 5147
Change Reason	Upgrade
Change Type	Minor (Normal)
Priority	High
Risk Level	Medium
Timing	Normal

Description

This critical patch resolves Trend Micro OfficeScan Firewall driver Privilege Escalation and Pool Corruption vulnerabilities. It also includes support for Windows 10 (version 1803) April 2018 Update.

OSCE XG SP1 Critical Patch	Build 5147 Download link
Release Date	2018-06-06
Size (MB)	352.5
Product Documentation	Critical Patch Readme link
Hotfixes included in OSCE XG SP1 Critical Patch Build 5147	http://files.trendmicro.com/products/officescan/XG/SP1/osce_xg_sp1_win_en_criticalpatch_5147.html#release
Network Traffic for Upgrading OfficeScan Agents	32-bit endpoint = 76.5 MB 64-bit endpoint = 108.4 MB
Requires Reboot after installation	Yes (All Endpoints)

Files Included in this release	
A. Files for Current Issue(s) ---------- Filename Build Number ---------- ---------- OfficeScan\PCCSRV\ ---------- CGIResUTF8.dll 12.0.0.5147 libNetCtrl.dll 13.0.0.5137 OfcPfwCommon.dll 13.0.0.5137	OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\common\ ---------- js-clientmag.js ln_cloud.js ln_common.js trend-ui.domaintree.js trend-ui-opt_list.js OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\common\l1

OfcPIPC.dll 13.0.0.5137
ofc_loadhttp.dll 13.0.0.5137

OfficeScan\PCCSRV\Admin\

InstNTRes.dll 12.0.0.5147
SetupUsr.dll 12.0.0.5147
ofc_loadhttp.dll 13.0.0.5137

OfficeScan\PCCSRV\Admin\Utility\ClientPackager\

OfcPfwCommon.dll 13.0.0.5137

OfficeScan\PCCSRV\Admin\Utility\EdgeServer*.*

OfficeScan\PCCSRV\Admin\Utility\PolicyExportTool\

CGIResUTF8.dll 12.0.0.5147

OfficeScan\PCCSRV\Admin\Utility\SaasStorageMgr\
---
ofcASMgr.exe 12.0.0.5147

OfficeScan\PCCSRV\Admin\Utility\SQL*.*

OfficeScan\PCCSRV\Admin\Utility\SQL\
---
libSQLDatabaseUpgrade.dll 12.0.0.5147
oscedbt.exe 12.0.0.5147

OfficeScan\PCCSRV\Admin\Utility\ServerMigrationTool\

CGIResUTF8.dll 12.0.0.5147

OfficeScan\PCCSRV\Admin\Utility\TMVS\

TMVS.exe 12.0.0.5147

OfficeScan\PCCSRV\CmAgent\

CGIResUTF8.dll 12.0.0.5147
ProductLibrary.dll 12.0.0.5147
ProductUI.zip

OfficeScan\PCCSRV\Download\Engine\

BMdriver_x32.sig
BMdriver_x32.zip
BMdriver_x64.sig
BMdriver_x64.zip
bmservice_x32.sig
bmservice_x32.zip
bmservice_x64.sig
bmservice_x64.zip

OfficeScan\PCCSRV\Download\Product\

DlpLite_Common.zip
DlpLite_Common_x64.zip

OfficeScan\PCCSRV\Engine\

TmAegisSysEvt.dll 2.976.0.2152
TMBMCLI.dll 2.976.0.2152
TMBMSRV.exe 2.976.0.2152
tmcomeng.dll 2.976.0.2152
TmEngDrv.dll 2.976.0.2152
TMPEM.dll 2.976.0.2152

0n\
---
l10n.clientmag.js
l10n.dlp.js
l10n.global.js
l10n.logs.js
l10n.update.js

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\common\cs
s\
---
index.css
l10n-style.css

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\common\ut
il\
---
common.js
sce.menubar.js

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\compliance
_report\
---
compliance_report.htm

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\dlp\
---
dlp_FileAttr_addedit.htm

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\logs\
---
logs_pfw.htm
logs_pfw_detail.htm
logs_pfw_view.htm
logs_trendx_view.htm

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\serveradm\
---
edge_server.htm
server_cmagent_saas.htm
server_migration.htm
server_proxy.htm

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\root\
---
help_start.htm
logon.htm
menu.html

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\outbreak\
---
opp_mutex_block.htm

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\widget\-
---
osce_proxy.php

OfficeScan\PCCSRV\Web_OSCE\HTML\widget\repository\widget
Pool\product\
---
config.php

OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\tools\
---
tools_admin_clients.htm

OfficeScan\PCCSRV\Web_OSCE\Web_Console\RemoteInstallCGI
\

tmtap.dll	6.0.0.1074
tmwlutil.dll	2.976.0.2152
TmPfw.exe	5.83.0.1050
TmPfwApi.dll	5.83.0.1050
TmSysEvt.dll	7.0.0.1160

OfficeScan\PCCSRV\Engine\x64\

TmAegisSysEvt.dll	2.976.0.2152
TMBMCLI.dll	2.976.0.2152
TMBMSRV.exe	2.976.0.2152
tmcomeng.dll	2.976.0.2152
TmEngDrv.dll	2.976.0.2152
TMPEM.dll	2.976.0.2152
tmtap.dll	6.0.0.1074
tmwlutil.dll	2.976.0.2152
TmPfw.exe	5.83.0.1050
TmPfwApi.dll	5.83.0.1050
TmSysEvt.dll	7.0.0.1160

OfficeScan\PCCSRV\LWCS\

lwcs_msg.ini	

OfficeScan\PCCSRV\Pccnt\

NTMonRes.dll	12.0.0.5147

OfficeScan\PCCSRV\Private\

DlpClc.xml	

OfficeScan\PCCSRV\Private\certificate\

libeay32.dll	1.0.2.12
openssl.exe	
ssleay32.dll	1.0.2.12

OfficeScan\PCCSRV\Web\Service\

AosProxy.exe	12.0.0.5147
CGIOCommon.dll	12.0.0.5147
CGIResUTF8.dll	12.0.0.5147
CmdHLClient.dll	12.0.0.5147
CmdHOConsole.dll	12.0.0.5147
cme_dll.dll	6.2.0.1196
cme_vxe_dll_static.dll	6.2.0.1196
DbServer.exe	12.0.0.5147
libCmdHndlrClientV2.dll	12.0.0.5147
libCmdHndlrConsoleV2.dll	12.0.0.5147
OfcDBBackup.exe	12.0.0.5147
OfcDownload.dll	12.0.0.5147
OfcNotifyQueue.dll	12.0.0.5147
OfcService.exe	12.0.0.5147
OfcCCCAUpdate.exe	13.0.0.5137
OfcPfwCommon.dll	13.0.0.5137
ofc_loadhttp.dll	13.0.0.5137
VerConn.exe	12.0.0.5147

OfficeScan\PCCSRV\Web_OSCE\Web\CGI\

cgiExportInfo.exe	12.0.0.5147
CGIResUTF8.dll	12.0.0.5147
OfcPfwCommon.dll	13.0.0.5137

OfficeScan\PCCSRV\Web_OSCE\Web_console\CGI\

cgiAuthManagement.exe	12.0.0.5147
cgiRemoteInstall.exe	12.0.0.5147
CGIResUTF8.dll	12.0.0.5147

OfficeScan\PCCSRV\Pccnt\Disk1*.*

OfficeScan\PCCSRV\Pccnt\Drv\

tmactmon.cat	
tmactmon.inf	
tmactmon.sys	2.976.0.2150
tmcomm.cat	
tmcomm.inf	
tmcomm.sys	7.0.0.1160
tmevtmgr.cat	
tmevtmgr.inf	
tmevtmgr.sys	2.976.0.2150
tmusa.cat	
tmusa.inf	
tmusa.sys	3.0.0.1047
tmwfp.cat	
tmwfp.inf	
tmwfp.sys	5.83.0.1051

OfficeScan\PCCSRV\Pccnt\Drv\X64\

tmactmon.cat	
tmactmon.inf	
tmactmon.sys	2.976.0.2150
tmcomm.cat	
tmcomm.inf	
tmcomm.sys	7.0.0.1160
tmevtmgr.cat	
tmevtmgr.inf	
tmevtmgr.sys	2.976.0.2150
tmusa.cat	
tmusa.inf	
tmusa.sys	3.0.0.1047
tmwfp.cat	
tmwfp.inf	
tmwfp.sys	5.83.0.1051

OfficeScan\PCCSRV\Pccnt\

ClientConsole.zip	
NTRtScan.exe	13.0.0.5137
NTMonRes.dll	12.0.0.5147

OfficeScan\PCCSRV\Pccnt\Common\

ApricotCBRuleHandler.dll	2.0.0.1033
ApricotManagerModule.dll	2.0.0.1033
CCSF_WIN32.zip	
CNTAoSMgr.exe	2.3.0.4516
crc0filter.dll	2.82.0.1056
fcWofieUI.dll	13.0.0.5137
FileBrowsingRuleHandler.dll	2.0.0.1033
ICRCHdler.dll	2.82.0.1056
libApricotLog.dll	2.0.0.1033
libNetCtrl.dll	13.0.0.5137
libcurl.dll	7.55.1.0
libeay32.dll	1.0.2.14
ssleay32.dll	1.0.2.14
NTRmv.exe	13.0.0.5137
OfcCCCAUpdate.exe	13.0.0.5137
OfcPfwCommon.dll	13.0.0.5137
OfcPfwSvc.dll	13.0.0.5137
OfcPIPC.dll	13.0.0.5137

cgiChkMasterPwd.exe	12.0.0.5147
CGIOCommon.dll	12.0.0.5147
CGIResUTF8.dll	12.0.0.5147
cgiShowActiveDirectory.exe	12.0.0.5147
cgiShowClientAdm.exe	12.0.0.5147
cgiShowLogs.exe	12.0.0.5147
cgiShowServerAdm.exe	12.0.0.5147
cgiShowSummary.exe	12.0.0.5147
cgiShowUpdate.exe	12.0.0.5147
fcgiOfcDDA.exe	12.0.0.5147
OfcPfwCommon.dll	13.0.0.5137
OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\aegis\	
---	---
device_control.htm	
OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\Auth\	
---	---
admin_account_info.htm	
admin_account_menu.htm	
Admin_Role_Add.htm	
Admin_User_List.htm	
OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\behavior_monitoring\	
---	---
bm_settings.htm	
OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\clientmag\	
---	---
client_cfg_wtp.htm	
client_globalsetting.htm	
client_list_2.htm	
client_urlfiltering_profiles.htm	
install_remote.htm	
OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\cloud_service\	
---	---
import_bw_list.htm	
scan_source.htm	

ofc_loadhttp.dll	13.0.0.5137
PccNT.exe	13.0.0.5137
PccNTMon.exe	13.0.0.5137
TmListen.dll	13.0.0.5137
Tmlisten.exe	13.0.0.5137
TmListenShare.dll	13.0.0.5137
TmPfw.exe	5.83.0.1050
TmPfwApi.dll	5.83.0.1050
TmPfwCtl.dll	5.83.0.1050
TmSock.dll	13.0.0.5137
TmSSClient.exe	13.0.0.5137
OfficeScan\PCCSRV\Pccnt\Win64\X64\	
---	---
ApricotCBRuleHandler.dll	2.0.0.1033
ApricotManagerModule.dll	2.0.0.1033
CCSF_X64.zip	
crc0filter.dll	2.82.0.1056
fcWofieUI.dll	13.0.0.5137
FileBrowsingRuleHandler.dll	2.0.0.1033
ICRCHdler.dll	2.82.0.1056
libApricotLog.dll	2.0.0.1033
libNetCtrl_64x.dll	13.0.0.5137
libcurl.dll	7.55.1.0
libeay32.dll	1.0.2.14
ssleay32.dll	1.0.2.14
NTRmv.exe	13.0.0.5137
Ntrtscan.exe	13.0.0.5137
OfcCCCAUpdate.exe	13.0.0.5137
OfcPfwCommon_64x.dll	13.0.0.5137
OfcPfwSvc_64x.dll	13.0.0.5137
OfcPIPC_64x.dll	13.0.0.5137
ofc_loadhttp_64x.dll	13.0.0.5137
PccNT.exe	13.0.0.5137
PccNTMon.exe	13.0.0.5137
Tmlisten.exe	13.0.0.5137
TmListen_64x.dll	13.0.0.5137
TmListenShare_64x.dll	13.0.0.5137
TmPfw.exe	5.83.0.1050
TmPfwApi.dll	5.83.0.1050
TmPfwCtl.dll	5.83.0.1050
TmSock_64x.dll	13.0.0.5137
TmSSClient.exe	13.0.0.5137

Implementation, Test and Backout Plan

Implementation Plan
Installing OSCE XG SP1 Critical Patch build 5147: 1. Download the package from Trend Micro Download Center. 2. Copy the CriticalPatch executable file to a temporary folder on the server, for example, "C:\temp". 3. Double-click the file. The modules are automatically copied to the correct destination. 4. Functional verification of test plan Note: This Critical Patch installation package automatically rolls back the OfficeScan server to its previous configuration if there are problems during installation. If you encounter problems after installation, do a manual rollback.

Test Plan	Backout Plan
[OfficeScan Server] • Service pack installation completed without errors • OfficeScan console can be accessed without issue • OfficeScan settings are intact • All agents are showing in the console • All OfficeScan Server services are running [OfficeScan Agent] • All OfficeScan Client services are running • OfficeScan agent icon is present in the system tray without error • Can launch OSCE agent console	To manually roll back to the previous build: 1. Locate the backup folder that the Critical Patch package created in the "\PCCSRV\Backup\CriticalPatch_B5147 " directory. 2. Stop the OfficeScan Master Service. 3. Stop the OfficeScan CMAgent Service. 4. Copy the backup modules to the original folders. 5. Start the OfficeScan CMAgent Service. 6. Start the OfficeScan Master Service.

APPENDIX

Patch Type

Describes the types of fixes that are available to Trend Micro users.

Service Pack	Fix cumulative problems and add features
Patch	Fix cumulative problems and add features / parameters relating to problems
Critical Patch / Security Patch	Fixes to address urgent issues (including vulnerabilities)
Hotfix	Fixes to address specific issues
Debug Module	Special fixes and tools for investigating issues

Change Type (Impact)

Minor (Normal)	Minor changes are those that require 4 to 6 days to prepare to implement. The Change will have little or no effect to end users during working hours, but may require the service to be unavailable for less than 10 minutes during non-working hours.
Moderate	The Change may affect a moderate number of users, probably limited to a single branch or large user group and may require the service to be unavailable for longer than 10 minutes or have a visible change to end users.
Significant	Significant are those that require 7 or more days to prepare to implement, or require a system outage of any kind. The Change may affect a single Ministry or several branches across multiple Ministries and may require the service to be unavailable for longer than 10 minutes or have a visible change to end users.

Priority

Low	A Change that impacts few users, and can be implemented in the long term
Medium	A Change that impacts a moderate number of users, and can be implemented in the medium-term
High	A Change that impacts a significant number of users, and must be implemented in the short term (Immediately)

Risk Level

Low	Routine change with proven success; minimal impact if Change fails; no back out required or back out is simple
Medium	High probability of success; back out is involved but not difficult; moderate visibility potential to customers
High	Change is complex or high risk; implementation is difficult; back out is lengthy and/or difficult; high visibility potential to customers.

Timing (Class)

Normal	Default timing for a change. Submitted greater than 5 days ahead of planned change. (Will require Manager Approval)
Emergency	Submitted greater than 5 days ahead of planned change. (Will require Manager Approval)