Security Management System Release Notes

Version 4.4.0 Patch 1

September 2016

This document contains release-specific information for the TippingPoint Security Management System (SMS). The release notes describe changes included in this release. This document is intended for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint SMS appliances and associated devices.

To ensure that you have the latest version of the release notes and other product documentation, download these documents from the Threat Management Center (TMC) at *https://tmc.tippingpoint.com*, or contact your TippingPoint representative.

This document contains the following important information:

New and changed in this release

This document contains information on issues and updates specific to SMS v4.4.0 Patch 1. Refer to the SMS v4.4.0 release notes located on the TMC for information on new features and content in the SMS v4.4.0 release.

This patch release includes several fixed issues, described in *Resolved issues* on page 3.

Installation

For installation instructions, refer to the *Install your appliance* documents on the TMC.

Important: You must upgrade to SMS v4.4.0 before you upgrade to SMS v4.4.0 Patch 1.

Upgrading to SMS v4.4.0

We recommend that you have SMS v4.1.0 or later installed before you upgrade to SMS v4.4.0.

You can upgrade the client automatically from SMS v4.3.0 to v4.4.0. However, if you upgrade directly from v4.2.1 or earlier to v4.4.0, you need to download the client manually.

Installing the SMS client on a Mac OS X computer

Before you install the SMS client on a Mac OS X computer, you must install Java 8 Runtime. An SMS client that runs on a Mac with Oracle Java Runtime version 1.8u71 or later will not connect to an SMS that still runs with a 1K certificate key. (111633, 112699)

Workaround: Change the SMS to use the 2K certificate key. Go to **Admin** > **General** > **SMS Certificate Key** to upgrade to a 2K key. For more information, see the *SMS v4.4.0 release notes* on the TMC.

Upgrading to SMS v4.4.0 Patch 1

This patch can be deployed on any system with SMS v4.4.0 installed.

Note: Before you apply this patch, break SMS HA and then apply the patch to both systems. Once the patch is installed on both systems, re-establish HA. For more information on HA, see the *TippingPoint Security Management System User Guide.*

Important installation information

- During installation, the SMS client will become unresponsive. Do not cancel the operation or reboot the SMS.
- After installing this patch, the SMS will restart. The installation and restart should take approximately 15 minutes.
- You will be prompted to update the SMS client after the patch is installed.
- If you uninstall then reinstall this patch, the SMS might not restart correctly. If this automatic restart fails, reboot the SMS.

Product version compatibility

The following table lists all compatible versions of the TippingPoint Virtual Protection System (vTPS), Threat Protection System (TPS), Intrusion Prevention System (IPS), Next Generation Firewall (NGFW), and Identity Agent devices with different SMS versions.

	SMS v4.4.0	SMS v4.3.0	SMS v4.2.0	SMS v4.1.0
vTPS	TOS v4.0.1	Not supported	Not supported	Not supported
TPS	TOS v4.1 and earlier	TOS v4.0.0	Not supported	Not supported
IPS	TOS v3.8.x and earlier	TOS v3.8.x and earlier	TOS v3.8.x and earlier	TOS v3.7.x and earlier
NGFW	TOS v1.2.3 and earlier	TOS v1.2.3 and earlier	TOS v1.1.1 and earlier	TOS v1.1 and earlier
Identity Agent	v1.0.0	v1.0.0	v1.0.0	Not supported

Resolved issues

The following items, grouped by category, provide clarification or describe issues fixed in this release.

Admin

Device	Description	Reference
vTPS, 440T	The SMS stopped sending all remote syslog events and stopped receiving packet capture (PCAP) files when the SMS received an IPS event from a TOS v4.0.1 device (vTPS or 440T).	113370
SMS	The SMS client interface was enhanced with an option that allows you to suppress the notification of used named objects. This enhancement enables you to quickly delete a large number of anonymous named objects.	113629

Client

Device	Description	Reference
SMS	The geographical maps in the SMS stopped working after a third party server discontinued the map data it provided to TippingPoint. These maps were found in certain dashboard gadgets and in the **Events** view. TippingPoint now receives map data from a different source.	113873

Devices

Device	Description	Reference
TPS, vTPS	When you attempted to create a virtual segment containing all physical segments on two or more devices, you could not add this virtual segment to all selected devices.	112623

Profiles

Device	Description	Reference
SMS, IPS	When you edited the IPS physical segment settings (i.e., Intrinsic Network High Availability and Link Down Synchronization), the SMS client may have displayed a RuntimeException error.	113273
SMS	If you activated a Digital Vaccine Toolkit (DV Toolkit) or Aux DV package and ran a query for **New DV Filters**, the results showed the new filters from the DV Toolkit or Aux DV package.	113533
SMS	For imported vulnerability scans, filter names did not show up in the CVE Search results, and the sorting function did not work.	113709
SMS	The Filter Taxonomy Criteria panel content was empty after the SMS was updated or a new DV was activated.	113835

Reputation

Device	Description	Reference
SMS	The date of imported Reputation User Provided Entries is based on the time-zone set on the SMS server, not the SMS client. The SMS correctly recognizes the time-zones specified in the reputation import file. **Note:** When the SMS server and the SMS client are in different time zones, it is a best practice to use the time-zone option in the input date format of the Tag Category. Enter the time-zone on the imported file of entries.	109210
SMS	IPv6 addresses that were deleted from the Reputation Database on the SMS were not always removed from the device.	113194

Known issues

This release contains the following known issues.

Admin

Device	Description	Reference
SMS	After a backup is restored, the status continues to show that the backup is in progress. **Workaround**: Ignore this status.	104680
SMS	If you upgrade the SMS from v4.3.0 to v4.4.0 while in FIPS mode and the same certificate is being used for both the remote system log and either LDAP or RADIUS, then the remote system log certificate will not appear. **Workaround**: To resolve this issue, re-import the certificate into the certificate store, and re-configure the certificate for the remote system log.	112430

Device	Description	Reference
SMS	After you click on the **Export and Archives** page in a web browser, the following message appears in the audit log each time you manage or delete a device: `Attempt to get a user group with id: SMS_EXPORT_ARCHIVE failed`. This may also occur when you import or delete DV Toolkit packages. **Workaround**: These messages do not affect functionality and can be ignored.	112837
SMS	SMS Client Communication protocols cannot be changed while in FIPS mode. For example, if you select TLS v1.1, and then go into FIPS mode, you will not be able to change the TLS version. **Workaround**: To change the TLS version, leave FIPS mode, make the change, and then go back into FIPS mode.	113000
IPS	After restoring a backup on the SMS, the TLS settings displayed all of the **SMS connecting to Device/TMC/LDAP** options as enabled, instead of how it was edited in the backup.	111789

Client

Device	Description	Reference
SMS	If you check the usages of multiple certificates on the SMS **Admin** > **Certificate Management** > **Certificates** or **CA Certificates** pages, non-specific device certificate usages may not be displayed if any of the certificates have a usage on the SMS (i.e. RADIUS, Web, etc.). **Note:** This does not affect certificates that have device usages such as User Authentication or VPN. **Workaround**: Check the usages of the individual certificates.	111547

Devices

Device	Description	Reference
SMS	When you create virtual segments, warning messages display in the **Validation Report** tab. However, the tab will still display as green even when there are warning messages. **Workaround**: Before you save a new virtual segment, check the **Validation Report** tab for warning messages, even if the tab is green.	108083
SMS	The VLAN ID range on the SMS and on the device LSM are not consistent. **Workaround**: Do not create a VLAN ID range that starts with 0 or ends with 4095.	108142
SMS	The check box to disable the Quarantine Automatically setting in the SMS does not work. **Workaround**: Disable the Quarantine Automatically setting through the LSM by navigating to **Policy** > **Settings** > **Quarantined Address** and selecting the check box **Automatically release quarantined address**.	112452
SMS	The SNMP and Authentication Preferences preview panels are not available to view in the Import Device Configuration Summary preview page before the configuration import settings are applied.	112520
SMS	If you manage a device with an SMS that does not have a certificate password, and you close or cancel the **Adding Device** dialog, you will get an error when you try to re-add the device that states that the device already exists in the SMS. This error will continue until the adding-device process completes. **Workaround**: When the **Adding device** dialog appears, do not close it; leave it open until it completes, or you receive an error message stating that you need to setup the password.	112590

Device	Description	Reference
SMS	When an inspection profile is distributed with an invalidly named SSL policy or SSL server to a user-defined virtual segment, the distribution fails. **Note:** The only valid characters are spaces, alphanumeric, and the following special characters: -, _, &, <, >, (,)	112724
IPS	When a virtual segment is reordered on the SMS, the following message may appear in the audit log for both affected and non-affected devices: `Update device virtual segment positions for devices <device name>`. **Note:** Only the devices associated with the reordered virtual segments are actually changed. **Workaround**: These audit log messages can be safely ignored on devices unassociated with the change.	112598
TPS	If the master-key for the TPS device is set with a device-specific key instead of a passphrase, the SMS does not show the system master-key information under **Device Configuration** > **Log Configuration**. Because of this, the SMS will not allow you to edit the configuration. **Workaround**: Do not use a device-generated key instead of a system master key to manage a device using the SMS.	111321
TPS	The SMS does not clearly indicate that a user role cannot be deleted because it is assigned to a user group. **Workaround**: Remove the user role from the user group that references it, then delete the user role.	111985
TPS	If a device was previously managed by the SMS using TLSv1.1 or higher and was then changed to use TLSv1.0 only, the SMS will not be able to manage the device. **Workaround**: To be able to manage the device again, change the TLS setting back to v1.1 or higher, restart the SMS, or allow the 24 hour connection timeout to occur. To avoid this issue, use the LSM to change the TLS configuration to TLSv1.0 when TLSv1.1 or higher was previously set.	112536

Device	Description	Reference
vTPS	The NGFW mode in vTPS does not support Jumbo frames, and the MTU value cannot be set higher than 1500. The MTU value is fixed and cannot be modified.	112230
vTPS	The SMS fails to distribute a reputation filter to the vTPS. **Workaround**: Perform a full synchronization of the Reputation database (from the SMS Profiles navigation pane, click **Reputation Database** > **Edit** > **Full Sync**).	112589
2200T	If two or more different SSL policies are using two different SSL servers and running the same certificate, when you distribute a profile that deletes these SSL policies, the SMS will: • Distribute the profile • Display an error on the distribution dialog • Log a message in the SMS syslog **Workaround**: Delete each SSL policy separately and distribute the policy to the device before you delete the next policy.	113249
IPS, NGFW	LSM users cannot be forcibly logged out from the SMS. **Workaround**: There is no workaround. However, LSM users are automatically logged out after a period of idleness (15 minutes) and when managed by the SMS, an LSM user has a read-only view that cannot modify the device configuration.	101042
SMS, NGFW	When you configure PPP interfaces (PPTP, PPPoE, L2TP), it is not possible to remove the password without removing the user. **Workaround**: To remove the password, remove the user ID.	104416
SMS, NGFW	You can create a device user group with a role of "none." This role has no capabilities.	105107

Device	Description	Reference
NGFW, vTPS	When you upgrade to a 2K certificate key on the SMS, the SMS Certificate Key Upgrade Wizard shows a warning message that the device is incompatible. This occurs with NGFW v1.2.2 and vTPS v4.0.1 devices. **Workaround:** When the SMS is managing a device with one of the above versions, disregard the warning message. Continue to upgrade to the 2K key by clicking **Next**, and then restart the SMS.	112773, 112842
vTPS, TPS	The Device SLG page does not correctly display the state of Performance Protection mode.	113132

DV Toolkit

Device	Description	Reference
SMS	When you override DV Toolkit Packages and distribute them to the device, the filter names in the DV Toolkit package on the device are different from the filter names that display on the SMS. For example, if a DV Toolkit package has a filter named `C031 Snort Rule`, the device displays the filter name as `C1000001 Snort Rule`.	105570
SMS	When you distribute a DV Toolkit package, the device system log shows a different package ID than is shown in the SMS system log. **Workaround**: The device system log reflects the merged packet ID. This discrepancy can be ignored because there is no functional impact.	106097
SMS, NGFW	You may notice a version error and exception when you distribute the same DV Toolkit package to NGFW devices in a cluster. **Workaround**: Uninstall the DV Toolkit packages from the devices, and then click **Sync Configuration Now**.	105136

Events

Device	Description	Reference
SMS	You cannot save an IPS event query when the firewall profile is included in the query.	105963
SMS	Instead of displaying the segment name, the interface grid under **Events** > **SSL sessions** appears as ethernetX.	113102
IPS	The SMS has problems synchronizing the URI metadata for events in the alerts table because the device sends URI metadata in two separate logs. As a result, the URI metadata may not be available for some events.	101575

Profiles

Device	Description	Reference
SMS	When you uninstall a Malware Filter Package from devices, the DV Inventory screen incorrectly reports that the uninstall failed on one device. **Workaround**: This display issue can be safely ignored. Logging out and logging back in will show that the package is removed from all devices.	105246
SMS	A refresh issue makes it appear that the Malware Filter Package Update allows more than one Malware Filter Package to be active. **Workaround**: This display issue can be safely ignored. Logging out and logging back in will show that only one package is active.	105344
SMS	A `UserNotAuthorized` error occurs when an administrator deletes the shared profile after the SuperUser deactivates the DV Toolkit package. **Workaround**: A SuperUser should delete the profile.	106231

Device	Description	Reference
SMS	When an Admin user copies a profile using a **Save As** operation, the Admin user will not have access to the copied profile until a SuperUser gives the Admin user access. **Workaround**: The SuperUser can give the Admin user access to the copied profile. Alternatively, the Admin user can access the profile by exporting and then importing it.	106325
SMS	When you try to export/import a profile from one SMS to another SMS, and when either or both of them are in FIPS mode, the selected SMS does not become available, and the export/import fails. **Workaround**: Export the profile to a local file, and then import it into the SMS.	106570
SMS	When a profile is imported from a device segment group, sometimes the active profile version does not match what is shown in the **Details** screen display. **Workaround**: Log out and log back in to the SMS for the version numbers to display correctly.	108034
SMS	A foreign key-constraint error sometimes appears in the SMS system log during an AUX DV package activation. **Workaround**: This error message can be safely ignored.	108055
SMS	When you use the **Overwrite** option while you activate a DV Toolkit package, the SMS displays the installed devices of the previously active DV Toolkit instead of the devices for the new DV Toolkit. **Workaround**: Distribute the current ACTIVE CSW.	108137
SMS	When an SSL policy is deleted through the SMS, the SSL profile and server are deleted, but sometimes the certificate is not deleted. **Workaround**: Delete the certificate manually through the LSM.	108971
SMS	When a profile is distributed using a schedule, the version of the profile is displayed as "null" or is missing in the audit log.	112217

Device	Description	Reference
	Workaround: Distribute the profile on demand using the UI to display the correct version.	
SMS	When you attempt to modify an inherited SSL inspection policy, the policy will no longer be visible, but if you log off and log back into the SMS, the policy will reappear in the child profile. Changing the parent policy no longer changes the state of the child policy, but the SSL server validation of the parent profile will still take into account the state of the SSL server of the child policy, which might cause the SSL server validation to fail.	113117
SMS	When an inspection profile has an SSL policy and any option selected as the destination IP address in a DDoS filter, the SMS displays an error message. **Workaround**: Use 0.0.0.1/0 for the **Any** selection in the DDos filter.	113245
SMS	When you remove a single list value from a tag category, the SMS will remove the tags from the user entry categories that use that tag. **Workaround**: Export the user entries from the SMS, edit them, and then re-import them on the SMS. Alternatively, you can also make a new tag category with the list values.	113302
TPS	If the SMS is running a DV that is older than 4.0 when you activate a vTPS DV (DV version 4.0), the complete DV will be re-loaded instead of just signatures with an updated iteration ID. This DV activation will take longer and will also reset any user-configured policy parameters for Scan and Sweep filters.	108614
IPS	Using non-ASCII characters in a profile description may cause problems on the device.	112910

Reports

Device	Description	Reference
SMS	When you generate an executive report, the event query will display an inaccurate query structure.	103620
SMS	When you generate a Specific Country report (**Inspection** > **Security** or **Inspection** > **Application**), or when you generate an Inspection report (Security or Application) and the report has country criteria, if you click a link in the report, you cannot use the **Refresh** button on the Events panel until you restart the SMS client.	106322

Reputation

Device	Description	Reference
SMS	The progress window that displays during a Reputation Database Full Sync does not update and will only show that the sync is "In Queue". **Workaround**: Click on the **Reputation Database** > **Activity** tab to verify the actual progress.	108870

Web API

Device	Description	Reference
SMS	A user can export and distribute a profile to a device or segment without the proper access to those profiles, devices, or segments.	108052
SMS	When you run a position update on a virtual segment with a number that exceeds the number of segments on the list, an `Unexpected Error Occurred` message is returned.	108182

Device	Description	Reference
SMS	When there are duplicate VLAN IDs in an XML file and you use the Web API virtual segment Create command, an unexpected error occurs. **Workaround**: Do not duplicate VLAN IDs in the XML file when you create virtual segments.	108184
SMS	The profile name does not display in the SMS audit log message when a profile is distributed through web services.	108197
SMS	An error message is displayed if virtual segments with the same name are sent to a device.	108267

Contacting support

Contact the TippingPoint Technical Assistance Center (TAC) by using any of the following options.

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

International: See *https://tmc.tippingpoint.com*

Legal and notice information

Trend Micro Incorporated makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro Incorporated shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Trend Micro Incorporated. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro Incorporated products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro Incorporated shall not be liable for technical or editorial errors or omissions contained herein.

TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their respective owners. This document contains confidential information, trade secrets or both, which are the property of Trend Micro. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Trend Micro or one of its subsidiaries.

All other company and product names may be trademarks of their respective holders.

Edition: September 2016

Publication Part Number: B09152011