Security Management System Release Notes

Version 4.3.0 Patch 2

Release date: July 2016

This document contains release-specific information for the TippingPoint Security Management System (SMS). The release notes describe new features and 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:

Installation

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*.

This patch can be deployed on any system running SMS v4.3.0 or SMS v4.3.0 Patch 1. For installation instructions, refer to the *TippingPoint Security Management System (SMS) User Guide* located on the TMC, *https://tmc.tippingpoint.com/TMC/*.

Important installation information

- During the installation, the client will become unresponsive - do not cancel the operation or reboot the SMS.

- After you install or roll back to this patch, the SMS will reboot. This process should take approximately 15 minutes to complete.
- You will be prompted to update the SMS client after the patch is installed.

Resolved issues

The following items provide clarification or describe issues fixed in this patch.

Admin

Device	Description	Reference
SMS	The SMS did not log failed Active Directory login attempts in the SMS audit logs.	112975
SMS	When you configured a UDP syslog server, if the DNS hostname became invalid and then valid, the SMS did not send the entries to the syslog server.	111792
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	Security issues were fixed for CVE-2016-0777 and CVE-2016-0778.	109196

Database

Device	Description	Reference
SMS, NGFW	The SMS did not display NGFW block or permit event notifications.	104371

Devices

Device	Description	Reference
SMS	The SMS became unresponsive because of a memory issue.	108199
SMS	The SMS used too many connections to manage devices, which resulted in memory and performance issues.	107447
IPS	The SMS sometimes failed when bulk-managing IPS devices that had an error about a duplicate SHORT_ID.	107561
NGFW, TPS	Managed NGFW and TPS devices on the SMS did not always refresh.	109120

Identity Agent

Device	Description	Reference
Identity Agent	The SMS might lose Identity Agent events for customers using languages that require the utf-8 character set.	111454

Events

Device	Description	Reference
SMS	The SMS did not send event notifications to all configured Remote Syslog servers.	111640

Profiles

Device	Description	Reference
SMS	Profile distribution sometimes caused certain filter overrides on other segments of the same device to revert to category settings.	108783
SMS, IPS	When you distributed a profile to an IPS device and then modified a user-defined service, the SMS and IPS became out of sync after the distribution was complete.	112356
SMS	When you distributed a Digital Vaccine Toolkit (DVT) to a device and reboot the SMS before the distribution process was complete, the SMS was not able to distribute the DVT to the device.	108846
SMS	When you created a profile that used the Hyper-Aggressive deployment mode, the SMS displayed an incorrect state (disabled) for the deployment mode.	112164

Reputation

Device	Description	Reference
SMS	The SMS allowed wildcards, such as a question mark and an asterisk, for a domain name. In this patch, when you create or edit domain name exceptions, you must explicitly list each domain name that you want to exclude from the filters. Wildcards will not work.	112196
IPS	When DNS entries that contained international domain names were imported, sometimes the SMS did not convert them correctly. This resulted in `Out of order IPDB database errors` on the IPS.	111925
SMS	A non-Reputation profile was distributed to a device with a FULL IPDB package and resulted in a device leak because the IPDB package contained zero entries.	112738

Device	Description	Reference
SMS	When the SMS marked the IPDB for a device as "out-of-sync", it marked every device as "out-of-sync." This caused a full IPDB for the next distribution.	112742
SMS	An IP address from a CIDR was excluded from a subnet range on Reputation filters.	109186
SMS	After a device was re-managed on the SMS, Reputation traffic for a segment leaked when a non-Reputation profile distribution replaced the Reputation profile on a different segment.	113271

Responder

Device	Description	Reference
SMS	A Responder Policy that included an IPS Quarantine Action Set and the **Escalate to SMS Response Event** option was enabled but the SMS did not display all of the quarantine log entries.	107157

Web API

Device	Description	Reference
SMS	Prior to this patch, the API to get policy data returned incorrect results. For more information about the updates to the `getFilters` and `setFilters` servlets, see the *SMS External Interface Guide* located on the TMC, *https://tmc.tippingpoint.com/TMC/*	112762

Issues fixed in previous patches

This patch is cumulative and includes all of the issues fixed in the following previous patches:

- *SMS 4.3.0 Release Notes, Patch 1*

Known issues

This release contains the following known issues.

Admin

Device	Description	Reference
SMS	When the SMS is in FIPS Crypto Core mode, if you import an SMS Web Security SSL Certificate and then import a RADIUS certificate without restarting the SMS, the SMS will display a `NullPointerException` error message. **Workaround**: After you import an SMS Web Security SSL Certificate, restart the SMS before you import a RADIUS certificate.	101767
SMS	When the SMS is in FIPS Crypto Core mode, if you import an SMS Web Security SSL Certificate, the following certificate information will not be updated until you restart the SMS: • Subject DN • Valid After • Expires **Workaround**: Restart the SMS after you import an SMS Web Security SSL Certificate.	101302
SMS	After a backup is restored, the status continues to show that the backup is in progress. **Workaround**: This status can be ignored.	104680

Devices

Device	Description	Reference
SMS, NGFW	When you configure PPP interfaces (PPTP, PPPoE, L2TP), it is not possible to remove the password without removing the user.	104416

Device	Description	Reference
	Workaround: To remove the password, remove the user id.	
SMS, TPS	If you unmanage the device and then edit a user role in the LSM, the role capabilities do not display in the SMS when you remanage the device. **Workaround:** If you use the LSM to edit a user role that was originally created in the SMS, you must always use the LSM to edit that user role.	104684
SMS, NGFW	You can create a device user group with a role of "none." This role has no capabilities.	105107
SMS, NGFW	Sometimes after you reboot the NGFW appliance, the SMS client may still indicate that the NGFW is rebooting even though the reboot is complete. **Workaround:** Manually refresh the NGFW appliance by clicking the **Refresh** button in the SMS client.	105939
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	If you create or update a virtual segment in a device task and one of the devices is unmanaged, then an exception error might occur. **Workaround:** Do not create or update a virtual segment in a device task when one of the devices is not managed.	108269

DV Toolkit

Device	Description	Reference
NGFW	When you distribute a firewall profile to an NGFW appliance, a mismatch warning may display even though the SMS and NGFW appliance have the same DV Toolkit package. **Workaround:** This warning can be safely ignored.	104445
SMS	Depending on the number of DV Toolkit packages on the device, the Device Configuration (Management Information) may not display all of the package names. **Workaround:** You can see the complete list of DV Toolkit packages for the device on the Device Configuration Summary.	104856
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 from each NGFW device of the cluster, select the cluster on the Devices screen and click **Sync Con#guration Now**. Then redistribute the DV Toolkit packages back to each NGFW cluster device.	105136
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	After you import a new DV Toolkit package (with the **Activate the imported DV Toolkit package** check box selected to overwrite an existing, active filter package), the Device Summary screen does not display the name of the new DV Toolkit package. **Workaround:** After you distribute the overwritten DV Toolkit package to the device, the Device Summary screen will display the correct name of the package.	105789

Device	Description	Reference
SMS	The DV Toolkit package displays `unknown` on the DV Toolkit Distribute dialog box when you distribute a different DV Toolkit package to the device. `Unknown` displays because you do not have access to this package.	105846
SMS	Sometimes you must uninstall the DV Toolkit package twice for a DV Toolkit package to be uninstalled. **Workaround:** Uninstall the DV Toolkit package when there is no DV Toolkit distribution in progress.	105891
SMS	Sometimes if you have several individual DV Toolkit distributions happening to the same device at the same time on the SMS, some DV Toolkit packages may not be distributed to the device. When this happens, the Distribution Extended status does not list the DV Toolkit package that was not distributed to the device. This situation may also happen if you are uninstalling multiple DV Toolkit packages from the same device. **Workaround:** Select multiple DV Toolkit packages (instead of individual DV Toolkit packages) and then redistribute the packages to the device.	106058, 106350, 105492
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	When you distribute a DV Toolkit package that has several filter overrides, an `isValid: Signature` message displays in the device log if there are differences between the profile and DV Toolkit package. **Workaround:** Uninstall the DV Toolkit package from the device and redistribute the DV Toolkit package to the device. Then redistribute the profile. If you are unable to uninstall the DV Toolkit package from the device, restart the SMS client.	106236

Events

Device	Description	Reference
SMS	You cannot save an IPS event query when the firewall profile is included in the query.	105963

Profiles

Device	Description	Reference
NGFW	After you import a Reputation profile from an NGFW appliance, the SMS displays an error when you attempt to edit or distribute a Reputation filter. When you perform a filter search, the Reputation filter does not display in the profile filter summary or the profile search results. **Workaround:** Create a new Reputation profile with reputation entries in the SMS.	105008
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	When you import a profile from a device that has nonstandard service ports, the SMS updates inspection services for each profile and changes the version and modified dates for all the profiles on the SMS.	105964
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.	106325

Device	Description	Reference
	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.	
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 you import an existing profile name, it is invalid if it has the same name as another profile but uses a different case. However, a warning conflict does not appear to let you know that the name is invalid before you import the profile. Instead, the following error message appears: `The Profile could not be imported. An unexpected error occurred while trying to import the profile.` **Workaround:** When you import a profile, rename it if it is has the same name as another profile.	108260

Reports

Device	Description	Reference
SMS	When you generate an executive report, the event query will display an inaccurate query structure.	103620

Device	Description	Reference
SMS	After you create a report schedule you cannot make modifications to the schedule. **Workaround:** Delete the existing schedule and create a new schedule with modified criteria.	105349
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

Web API

The following issues are related to the new feature, Web API, described in the section .

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
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	When a device is removed from a virtual segment, the SMS response does not include the device name on the device result.	108265

Device	Description	Reference
SMS	An error message is displayed if virtual segments with the same name are sent to a device.	108267
SMS	The Web API `Update Virtual Segment` command does not allow you to rename the virtual segment. **Workaround:** Use the SMS client to rename the virtual segment.	108270

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

Edition: July 2016