Security Management System Release Notes

Version 4.4.0 Patch 2

Release date: January 2018

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:

- *New and changed in this release* on page 1
- *Resolved issues* on page 2

New and changed in this release

This document contains information on issues and updates specific to SMS v4.4.0 Patch 2, described in *Resolved issues* on page 2.

Issues fixed in previous patches

This patch is cumulative and includes all of the issues fixed in the previous patch. For information on the features in SMS v4.4.0, refer to the SMS documentation located on the TMC at *https://tmc.tippingpoint.com/*.

Important note for users of the SMS Web API authenticating with URL encoded credentials

This patch changes what data SMS debug logs include when logging web access requests to exclude those credentials. For details on this change and best practices, refer to *PB#1071*.

Important notes for SMS

- Patch installation should take approximately 15 minutes. During installation, the SMS client will become unresponsive; do not cancel the operation or reboot the SMS. The SMS Server will automatically reboot after the patch is installed. You will then be prompted to update the SMS client.
- A patch may be rolled back or uninstalled to the previous version.
- If your SMS system is operating in High Availability (HA) mode, you are no longer required to break HA to apply this patch.

Resolved issues

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

Profiles

Device	Description	Reference
SMS	Locks that got automatically placed on the Reputation Database during a profile distribution failed to be released. Copies of the locked database would then remain on the file system after a new database package was downloaded. This caused the size of each SMS backup to increase inordinately. The Reputation Database lock release mechanism has been repaired.	112040

Responder

Device	Description	Reference
SMS, IPS	An inability to identify whether a permitted address was configured in a hidden action set caused the IPS Quarantine action to stop sending new automatic quarantines. This patch resolves this issue.	116290
SMS, IPS	A quarantine cleanup agent did not work properly with the Active Responder History. This caused the Responder queue to get filled up and to stop sending quarantine actions to the IPS.	113704

Device	Description	Reference
	This patch repairs the cleanup issue and enables Responder to issue and remove quarantines during the cleanup.	

Product support

Information for you to contact product support is available on the TMC at *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 in any form or by any means, 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.

Edition: January 2018