Software Vulnerability Manager Release Notes
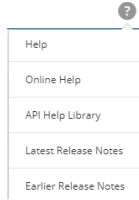
August 2018

Introduction

Software Vulnerability Manager reimagines how software is secured by closing the gap between IT Security and IT Operations by providing industry leading security research, risk assessment and remediation through Software Vulnerability Manager's key components:

- **Research:** Keep up with the latest software vulnerability research and advisories from Secunia Research

- **Assessment:** Discover where software vulnerabilities are installed across your organization

- **Patching:** Remediate software vulnerabilities in third-party applications

New Features and Enhancements

The following table lists new features and enhancements for Software Vulnerability Manager. The Affected Module(s) column refers to the specific Software Vulnerability Manager module(s) affected by the new feature or enhancement.

Affected Module(s)	Feature or Enhancement Description	Reference Number
Notifications	Software Vulnerability Manager release notes are now sent to administrators within the Notifications UI. To filter for release notes, select **News** under the Notifications **Type** filter.	SVM-418
Settings, Online Help	A Workflow Management rule and trigger were created to notify non-administrators of the latest Software Vulnerability Manager release notes. For the online help reference, see Create a Workflow Rule to send a new release notes notification to non-administrators.	SVM-419
Settings, Online Help	Software Vulnerability Manager's agent for Windows (Vulnerable Software Discovery Tool for Windows) now detects Windows updates against the SCCM database and from the Client Windows Update Agent for an enhanced vulnerability assessment. For the online help reference, see Microsoft Update Options.	SVM-705
Settings	Under **Settings > Assessment > Scan Configuration**, the default agent scan interval was changed from 300 (5 minutes) to 7200 (2 hours) to spread out scan executions and to optimize network performance.	SVM-766

Affected Module(s)	Feature or Enhancement Description	Reference Number
Online Help	Software Vulnerability Manager online help now uses secure https links. Note the following new links, which can be accessed in the upper-right-hand corner of the user interface. **Software Vulnerability Manager Help Library:** https://helpnet.flexerasoftware.com/svm/Default.htm **Software Vulnerability Manager API Help Library:** https://helpnet.flexerasoftware.com/svm/api/Default.htm **Latest Release Notes:** https://helpnet.flexerasoftware.com/?product=Software%20Vulnerability%20Manager&version=Current **Earlier Release Notes:** https://helpnet.flexerasoftware.com/?product=Software%20Vulnerability%20Manager&version=Previous	SVM-791

Resolved Issues

The following table lists resolved issues for Software Vulnerability Manager. The Affected Module(s) column refers to the specific Software Vulnerability Manager module(s) affected by the resolved issue.

Affected Module(s)	Issue Summary	Reference Number
Assessment	The Mac OS X Agent has been updated to be able to read binary plist (property list) files. This new ability to scan for additional software details may result in the detection of an increased number of software titles. It is recommended that you upgrade to this improved version of our Mac OS X Agent (Vulnerable Software Discovery Tool for Mac Version 8.0.337) under **Settings > Assessment > Downloads**.	SVM-768
Vulnerability Manager	Under **Vulnerability Manager > Watch Lists & Advisories > Watch Lists** you can create Assessment watch lists under the Assessment tab. If you edit the Confidentiality Requirement (CR), Integrity Requirement (IR), or Availability Requirement (AR) scores for Assessment watch lists listed under **My Assessment** and save them, the watch list's products and vendors will not be affected.	SVM-774

Affected Module(s)	Issue Summary	Reference Number
Online Help	Clarified in online help that the Software Distribution Daemon for Windows does not need to be installed on WSUS. For details, see Download and Install the Software Distribution Daemon for Windows.	SVM-776
Dashboard	The Dashboard widget **Most prevalent EOL software installations** now counts only End-of-Life (EOL) products instead of the total number of products found on the devices.	SVM-805

Product Feedback

Have a suggestion for how we can improve this product? Please come share direct feedback with the product team and vote on ideas submitted by other users in our Customer Community feedback page for Software Vulnerability Manager.

System Requirements

Software Vulnerability Manager's User Interface will resize and adapt when being used on different devices. You can access the system from anywhere using any device, such as a smartphone or tablet, running Internet Explorer 11 or higher, Chrome, Opera, Firefox, Safari and mobile browsers with an Internet connection capable of connecting to https://app.flexerasoftware.com.

Legal Information

Copyright Notice

Copyright © 2018 Flexera.

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/producer/company/about/intellectual-property/. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

Disclaimer

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. The provision of such information does not represent any commitment on the part of Flexera. Flexera 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. Flexera 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.

The software described in this document is furnished by Flexera under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software, except as specifically allowed in the license agreement. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to: photocopying, recording, or information recording and retrieval systems, for any purpose other than the purchaser's personal use, without the express, prior, written permission of Flexera.