

# Software Vulnerability Manager Release Notes

December 2017

<b>Introduction</b> .....	<b>1</b>
<b>New Features and Enhancements</b> .....	<b>2</b>
<b>Resolved Issues</b> .....	<b>4</b>
<b>Product Feedback</b> .....	<b>6</b>
<b>System Requirements</b> .....	<b>7</b>
<b>Legal Information</b> .....	<b>7</b>

## 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
- **Patching:** Remediate software vulnerabilities in third-party applications
- **Assessment:** Discover where software vulnerabilities are installed across your organization

# 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
<b>Assessment, Settings</b>	<p>Software Vulnerability Manager now scans the Red Hat Enterprise Linux (RHEL) platform.</p> <p>Go to Software Vulnerability Manager's <b>Settings &gt; Assessments &gt; Downloads</b> to download the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and Vulnerable Software Discovery Tool for Red Hat Linux 7 RPM.</p> <p>For the online help reference, see: <a href="http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Scanning_Red_Hat_Enterprise_Linux__RHEL_.htm">http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Scanning_Red_Hat_Enterprise_Linux__RHEL_.htm</a></p>	SVM-1
<b>Assessment</b>	<p>Under <b>Assessment &gt; Products &gt; Product Details</b> added a label titled <b>Entry Created</b> to record when a Product is added to Software Vulnerability Manager.</p>	SVM-85

Affected Module(s)	Feature or Enhancement Description	Reference Number
<b>Assessment</b>	<p>Under <b>Assessment &gt; Devices &gt; Device List</b> the column order has been changed to:</p> <ul style="list-style-type: none"> <li>Device Name</li> <li>Platform</li> <li>OS Version</li> <li>System Score</li> <li>Secure Products</li> <li>Insecure Products</li> <li>EOL Versions</li> <li>Discontinued Products</li> <li>Last Scanned</li> <li>Inventory Source</li> </ul> <p>Under <b>Assessment &gt; Devices &gt; Device List</b> the filter order has been changed to:</p> <ul style="list-style-type: none"> <li>Device Name</li> <li>Platform</li> <li>OS Version</li> <li>Has EOL Versions</li> <li>Has Discontinued Products</li> <li>Days since last Scan</li> </ul>	SVM-192
<b>Assessment</b>	Assessment Reports have the new Flexera logo.	SVM-198
<b>All</b>	Email notifications have the Software Vulnerability Manager product logo.	SVM-200
<b>All</b>	In legal and copyright information, “Flexera Software” and “Flexera Software LLC” has been changed to “Flexera”.	SVM-264
<b>Vulnerability Manager, Settings</b>	When a user is removed from a user group’s Watch List, there is now a settings options asking if all enforced Watch List subscriptions should be removed from the remaining user group members.	SVM-301

# 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
<b>Analytics</b>	In <b>Analytics &gt; Devices</b> the pie graphs now have on-click filters. In <b>Analytics &gt; Products</b> the pie graphs can now be filtered.	SVM-14
<b>Settings</b>	The following API filters are now working: <ul style="list-style-type: none"><li>Asset list filters vendor_name and product_name<ul style="list-style-type: none"><li>Example: api/product-releases/?vendor_name=DigitByte Studio</li><li>Example: api/product-releases/?product_name=001 File Joiner And Splitter Pro</li></ul></li><li>Product_is_os filter is_os<ul style="list-style-type: none"><li>Example: api/product-releases/?is_os=true</li></ul></li><li>Products filter vendor_name<ul style="list-style-type: none"><li>api/products/?vendor_name=Welltek Software</li></ul></li></ul>	SVM-18
<b>Research</b>	Product data inconsistency has been resolved between Software Vulnerability Manager and databases SVM Research/VIM4/VT to identify orphaned products.	SVM-81
<b>Vulnerability Manager</b>	Export Product Versions for “all products” now generates a .csv file.	SVM-213
<b>Assessment</b>	Performance issues for more than 30,000 hosts was addressed to ensure accurate counts when filtering, sorting, and exporting advisory and product details.	SVM-238
<b>Assessment</b>	Under <b>Assessment &gt; Advisories</b> , the <b>Reset</b> button now clears the page’s filters and the <b>Assessment &gt; Advisories</b> page refreshes after the user navigates to other modules within Software Vulnerability Manager.	SVM-251
<b>Research</b>	Sorting is now working in ascending order for <b>Type</b> under <b>Research &gt; Product Database &gt; Product Versions</b> . The <b>Type</b> filter includes the options Software and Operating System. When sorting in ascending order, Operating System appears before Software.	SVM-254
<b>Analytics</b>	The number of levels of Organizational Unit (OU) restrictions have been removed for navigating Assessment Reports.	SVM-257

Affected Module(s)	Issue Summary	Reference Number
<b>Patching</b>	The <b>Package</b> filter option under <b>Patching &gt; Deployment</b> now resets properly after clicking <b>Reset</b> .	SVM-289
<b>Settings</b>	Under <b>Settings &gt; API &gt; XML Feeds</b> the URLs have been corrected under the <b>XML</b> column.	SVM-303
<b>Dashboard</b>	Devices from deleted accounts are no longer processing data, which create more accurate device counts.	SVM-306
<b>Patching</b>	Improved detection logic on 64 bit machines so that publishing 32 bit and 64 bit packages to a 64 bit machine no longer leads to extra product being installed.	SVM-308
<b>Settings</b>	“Asset List” references have been replaced with “Watch List” in Watch List email alerts and throughout <b>Settings &gt; Workflow Management &gt; Rules</b> .	SVM-309
<b>Patching</b>	Patches filtered by “Affecting My Environment” now include End-of-Life products.	SVM-314
<b>Settings</b>	Removed a duplicate verification object when deleting user accounts.	SVM-317
<b>Analytics</b>	User account created through a migration from VIM4 has a report with sorting by impact type, which Software Vulnerability Manager does not support.	SVM-318
<b>Patching</b>	7-Zip and Foxit Reader can now be seen in the Patching console.	SVM-321
<b>Patching</b>	Adobe Flash NPAPI v. 17.x is now appearing as a non-assessment patch on Windows Server 2012 and Windows Server 2016.	SVM-322
<b>Dashboard</b>	Links in the <b>Dashboard</b> module for <b>Most critical advisory affecting your security</b> now direct user to the appropriate information under <b>Assessment &gt; Advisories &gt; Advisory Details</b> .	SVM-326
<b>Settings</b>	Removing users from User Groups and saving the necessary changes no longer shuts down Software Vulnerability Manager.	SVM-331
<b>Settings</b>	User role permissions have been restricted so that non-administrators cannot delete Watch List Groups.	SVM-341
<b>Assessment</b>	Reports are now successfully generated in PDF format.	SVM-346
<b>Analytics</b>	Under <b>Analytics &gt; Reports</b> the <b>Add Research Report</b> and <b>Add Assessment Report</b> pages now load.	SVM-351

Affected Module(s)	Issue Summary	Reference Number
<b>Research</b>	The <b>BID References</b> link <a href="http://www.securityfocus.com/bid/101001">http://www.securityfocus.com/bid/101001</a> for NVIDIA Multiple Products Multiple Vulnerabilities - CVE-2017-6268 now works.	SVM-361
<b>Patching</b>	Fixed patching deployment for the Firefox browser.	SVM-370
<b>Online Help - Introduction</b>	Renamed the section “Account Basics” as “Getting Started with Software Vulnerability Manager”. For details, see: <a href="http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Getting_Started_with_Software_Vulnerability_Manager.htm">http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Getting_Started_with_Software_Vulnerability_Manager.htm</a>  Added the following subsections: <ul style="list-style-type: none"> <li>Logging on to Software Vulnerability Manager: <a href="http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Logging_on_to_Software_Vulnerability_Manager.htm">http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Logging_on_to_Software_Vulnerability_Manager.htm</a></li> <li>Download the Vulnerable Software Discovery Tool for Windows, Mac, and Red Hat Linux: <a href="http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Download_the_Vulnerable_Software_Discovery_Tool_for_Windows__Mac__and_Red_H.htm">http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Download_the_Vulnerable_Software_Discovery_Tool_for_Windows__Mac__and_Red_H.htm</a></li> </ul>	N/A
<b>Online Help - Dashboard</b>	Clarified that Flexera’s definition of End-of-Life (EOL) software may differ from a software vendor’s. For details, see: <a href="http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Dashboard.htm">http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Dashboard.htm</a>	N/A
<b>Online Help - Assessment Scenarios</b>	Updated the section Run Assessment from System Center Configuration Manager (SCCM) to reflect current practice. For details, see: <a href="http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Run_Assessment_from_System_Center_Configuration_Manager__SCCM_.htm">http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Run_Assessment_from_System_Center_Configuration_Manager__SCCM_.htm</a>	N/A
<b>Online Help - Settings</b>	Added the section Daemon Log File Size. For details, see: <a href="http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Daemon_Log_File_Size.htm">http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Daemon_Log_File_Size.htm</a>	N/A

## 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

The Software Vulnerability Manager 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 © 2017 Flexera. All Rights Reserved.

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.