Software Vulnerability Manager Release Notes

July 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
- **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
Assessment, Online Help	A **Research Created** date was added for each product under **Assessment > Products > Product Details** to document when a product was added to the Software Vulnerability Manager's vulnerability database. For the online help reference, see Product Details.	SVM-85
Settings, Online Help	To improve user account management, Single Sign-On (SSO) has been added under **Settings > User Management > Single Sign On**. For the online help reference, see Single Sign-On. ***Note*** • *The online help procedure is specific to the SSO provider Okta (SAML 2.0).*	SVM-377 and SVM-764
Patching, Online Help	Under **Patching > Tickets**, Patching tickets now include a list of affected devices to help determine ticket priority. For the online help reference, see: Patching Tickets.	SVM-696
Settings, Online Help	Under **Settings > Workflow Management > Rules** you can now select multiple broadcast groups when creating workflow rule notifications using email or SMS. For the online help reference, see: Create a Workflow Rule - Overview.	SVM-715
Assessment	Due to a change in how Microsoft identifies Office 365 patches, we have made a new change to accommodate this scenario. You may notice additional vulnerability detections for Office 365 as a result in this release.	SVM-720
Assessment, Online Help	Added clarification in the online help for the three scan type options to scan via local agents. For the online help reference, see: Scan Types.	SVM-728
API Help Library - Research	Added the PowerShell Script to Save All Advisories Within a Date Range to CSV. For the online help reference, see: Research Module API Information.	SVM-736

Affected Module(s)	Feature or Enhancement Description	Reference Number
API Help Library - Assessment	Added for how to query assessment data based on Smart Groups. For the online help reference, see: To query assessment data based on Smart Groups.	SVM-744
Online Help	Clarified in online help that users can log on to Software Vulnerability Manager with either their user name or email address (but the user name and email address must both be unique). For details, see Logging on to Software Vulnerability Manager.	SVM-790

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
Research	Until now, we have been adding a reference to MS Project Server for advisories that apply to MS Project to ensure visibility. Customer feedback has indicated this is problematic, so going forward you must now follow each individually. If you have had MS Project in your watch list and wish to also see MS Project Server, it will be necessary going forward to add it as a distinct additional product.	VTL-501

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

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.