

Software Vulnerability Manager Release Notes

December 2018

Introduction	1
New Features and Enhancements	2
Resolved Issues	2
Product Feedback	3
System Requirements	3
Legal Information	3

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
Settings	Under Settings > User Management > Single Sign-On (SSO) > IDP Configuration Instructions the Service Provider Metadata URL was added.	SVM-913
Online Help, API Help	Added an explanation to the online and API help that on May 18, 2018 Flexera's Secunia Research began entering all new CVSS scores using the v3 standard. After a CVSSv3 score is entered, the score appears in the User Interface (UI), API, XML, email notifications, and PDF reports. For Online Help details, see CVSSv3 Score . For API Help details, see CVSSv3 Score .	SVM-955
API Help - Research	Added a PowerShell Script to Query Historic Advisories by Product and Version .	N/A

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	Sorting columns in Products and Advisories has been resolved in the Assessment module.	SVM-919
All	Downloaded advisory PDF files are no longer truncated.	SVM-951
Online Help	Clarified in the Software Vulnerability Manager Quick Start Guide that Flexera's Software Vulnerability Manager uses the standard Time-Based One-Time Password Algorithm (TOTP) for token-based two-factor support, which is supported by applications like Google Authenticator or Duo by Cisco. For details, see Token-Based 2FA .	N/A

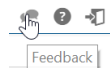
Product Feedback

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](#).



Note • You will need your Flexera Customer Community credentials to enter feedback.

You can also submit feedback through the Software Vulnerability Manager user interface by clicking the feedback icon in the upper-right-hand corner of each module.



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.