

Software Vulnerability Research Release Notes

May 2019

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





Introduction


Software Vulnerability Research 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 Research’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 Research. The Affected Module(s) column refers to the specific Software Vulnerability Research module(s) affected by the new feature or enhancement.

Affected Module(s)	Feature or Enhancement Description	Reference Number
Settings	Under Settings > Workflow Management > Rules , there is now an option to select Advisory Condition in the Choose Rule Trigger tab for Advisory channel	SVM-999
Settings	Under Settings > Workflow Management > Rules , there is now an option to select a trigger Advisory Threat for Watch List Changed in the Choose Rule Trigger tab for Advisory Channel.  Note • This add-on requires purchase of Threat Intelligence Module	SVM-999
Research	Under Research > Advisories you can see more details of threats associated with the exploits.  Note • This add-on requires purchase of Threat Intelligence Module	SVM-1017
Logo Change	Logo of Software Vulnerability Manager is changed to Software Vulnerability Research .	SVM-1018
Settings	Under Settings > Vulnerability Management > Watch List Subscriptions , there is now an option to Edit the Subscriber for existing watch list subscriptions.	SVM-1025
Analytics	Under Analytics > Reports , you can see the Threat Score details in the downloaded SAID's PDF file.  Note • This add-on requires purchase of Threat Intelligence Module	SVM-1030
Policy Manager	Under Policy Manager > Create New Policy , there is now an option to Set Policy Rule criteria based on Threat Score (Optional)  Note • This add-on requires purchase of Threat Intelligence Module	SVM-1031

Affected Module(s)	Feature or Enhancement Description	Reference Number
Email Notification with Threat Score	Under Settings > Workflow Management > Rules , if you select Advisory channel in the Choose Rule Trigger tab and select Email in the Add action tab, you can see Threat Score in the Email notifications.	SVM-1036
 <p>Note • This add-on requires purchase of Threat Intelligence Module</p>		

Resolved Issues

No resolved issues were included in this release.

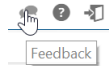
Product Feedback

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 Research](#)



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

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



System Requirements

Software Vulnerability Research'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 © 2019 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.