Software Vulnerability Manager (Cloud Edition) Release Notes

February 2021

Introduction

Flexera's Software Vulnerability Manager (formerly called Software Vulnerability Manager 2019) is a vulnerability and patch management software solution that facilitates a customized patch management process. It combines vulnerability intelligence, vulnerability scanning, and patch creation with patch deployment tool Integration to enable targeted, reliable, and cost-efficient patch management.

Vulnerability and patch management are critical components of any security infrastructure because they enable proactive detection and remediation of vulnerabilities before they are actively exploited and your security compromised. With Software Vulnerability Manager, IT operations and security teams are empowered to prevent vulnerability threats from both Microsoft and non-Microsoft (third-party) product vulnerabilities, covering Microsoft Windows, macOS, and Red Hat Enterprise Linux.

Software Vulnerability Manager integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager.

New Features and Enhancements

Software Vulnerability Manager (Cloud Edition) includes the following new features and enhancements:

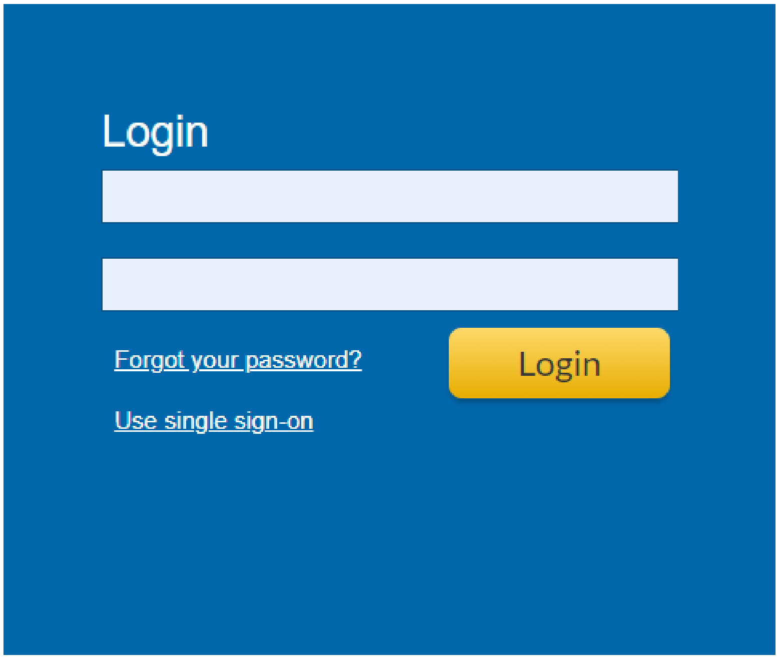
- Support for Service Provider Initiated Single Sign-On
- Other Enhancements/Improvements

- Binary Versions

***Note** • To see the following new features and enhancements in your Software Vulnerability Manager (Cloud Edition) interface, you must refresh your browser's cache (press Ctrl+F5).*

Support for Service Provider Initiated Single Sign-On

Software Vulnerability Manager Cloud Edition can now initiate Single Sign-On via Identify Provider for authentication. You can click on **Use single sign-on** on the SVM login page and then provide your official email address to be automatically redirected to the configured Identity Provider to initiate login process.



For more details, see Logging on to Software Vulnerability Manager Cloud Edition Using Single Sign-On.

Other Enhancements/Improvements

Following enhancements/improvements are added to SVM in this release:

- SVM-Intune Integration
    - SVM can now wrap multiple paths, used as detection rules for a package, into a single PowerShell Script and add it as a custom detection script, when a package is published to Microsoft Intune.
    - For few SVM packages, after the installation on an end point, the return code was not correctly sent back to Intune which resulted in incorrect deployment status of these packages in the Intune console. This issue is fixed now. Return code for all the packages are now sent back to Intune for accurate tracking of package deployment status.
- Patch Daemon

- Clicking on **Test SVM Connection** button in the **SVM Connection** tab of Patch Daemon, to generate a new token, upon its expiration, required the Patch Daemon service to be restarted for the connection to be successful. Patch Daemon is now enhanced to be more robust to handle new tokens, without the need to restart the service.

Binary Versions

Important • *For the current release, binary versions has not changed.*

The following are the version of the binaries provided:

Binaries (ActiveX/Agent/Daemon) version: 7.6.0.15

Software Vulnerability Manager Client Toolkit: v4.0.342 and above (download SVM Client Toolkit).

Resolved Issues

This release of Software Vulnerability Manager (Cloud Edition) does not include any resolved issues.

Community Blogs

Please subscribe to latest news on Software Vulnerability Manager by going to https://community.flexera.com/t5/Software-Vulnerability/bg-p/SoftwareVulnerabilityManagementblog and clicking on subscribe.

Product Feedback

Have a suggestion for how we can improve this product? Please share your feedback with the product team by visiting the Software Vulnerability Manager Forum in the Flexera Community:

https://community.flexera.com/t5/Software-Vulnerability/bd-p/SVM-Discussion

Legal Information

Copyright Notice

Intellectual Property

Restricted Rights Legend