Software Vulnerability Manager (Cloud Edition) Release Notes

April 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:

- SSO Integration with Azure
- Intune Enhancements
- 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).*

SSO Integration with Azure

In this update of Software Vulnerability Manager, you can integrate Azure SSO with SVM. This article explains how to configure SVM with Azure SSO.

Intune Enhancements

Following enhancements are added to Intune:

- Agent deployment via Intune.
- Addressed multiple bugs.
    - In some cases, patches may be applied even when the application was not present on the device, or an earlier version of the application was not present.
    - In some cases, when a targeted endpoint contained a newer version than the published version, the downgraded version was mistakenly being installed.
    - When the option to always install was selected for a patch, it would not always be applied to the target device as expected.
    - In some cases, SPS and VPM packages would not install to update as expected.

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

Version Updated:

Software Vulnerability Manager Client Toolkit: 5.0.XXX (download SVM Client Toolkit).

Known Issues

The following table lists the known issues in Software Vulnerability Manager (Cloud Edition):

Issue	Description
IOJ-2191902	Adobe Digital Editions 4.x showing wrong advisory mapping and criticality status in VPM view.
IOJ-2177891	Some applications do not appear when not installed to their default location. ● Java is often included with other applications. When vulnerable, the application that installed Java should be patched. Deploying a Java patch will only update/install Java to its standard location and will not patch the instance shipped with a third-party product. To avoid confusion and improper patching attempts, SVM intentionally scans for Java only in standard locations. ● If you would like to ensure known instances appear in scan results, you may choose to add a custom product in **Custom Scan Rules**. ● Choose **Custom Scan Rules** from the **Filter Scan Results** node under the Scanning menu. ● Click **New Custom Scan Rule**. ● Enter the name and browse the file that you wish to have appear in scan results.

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