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 (On-Premises Edition) includes the following new features and enhancements:

- **Patch Automation**
- **Import Bulk File Paths in SVM Patch Wizard**

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

Patch Automation

With this release of Software Vulnerability Manager, you can automate publishing of patches. To do so, right click on any SPS template or VPM patch and select **Subscribe to Patch** from the context menu.

![Selecting Subscribe to Patch from the Context Menu](image)

**Figure 1:** Selecting Subscribe to Patch from the Context Menu
On the **Configure Subscription** dialog box, you can choose to always publish a new patch when a new version becomes available, or you can choose to only automate publishing a new patch when certain criteria are met (recommended).

![Configure Subscription Dialog Box](image)

**Figure 2:** Configure Subscription Dialog Box

Patch automation is delivered via a new version of the Flexera SVM Patch Configuration (Version 2.x) tool, which is part of the Software Vulnerability Manager Client Toolkit. For more information on the toolkit, visit the [SVM Toolkit blog](https://resources.flexera.com/tools/SVM/SVMClientToolkitInstall.msi) in the Flexera Community.

The SVM Toolkit installer contains updates to the Flexera SVM Patch Configuration tool as well as some optional tools documented in our online community. The SVM Toolkit installer can be downloaded at:

https://resources.flexera.com/tools/SVM/SVMClientToolkitInstall.msi

Note • If you are already have the SVM Toolkit installed, the installer will upgrade you to the latest version.
You can see the status and details of patches published automatically on a new page named **Subscription Status**, which is opened by selecting **Subscription Status** on the **Patching** menu.

---

**Figure 3: Flexera SVM Patch Configuration Dialog Box**

**Figure 4: Subscription Status Page**
All the patch level activities are also recorded in the Activity Log, which is opened by selecting **Activity Log** on the **Configuration** menu.

**Figure 5: Activity Log Page**

In an upcoming release, Software Vulnerability Manager will also be introducing an option to get a daily/weekly activity digest via email.
Import Bulk File Paths in SVM Patch Wizard

To help with situations where you wish to include specific file paths for scanning software, you can now import multiple file paths by providing a CSV file during Step 3 of the patch/template creation process (CSIL-9630).

On the **Step 3 of 4: Applicability Criteria - Paths** panel, click **Add Path** to open the **Import Path Applicability Rules for Package** dialog box, and select a local CSV file which contains file paths.

![Import Path Applicability Rules for Package Dialog Box](image)

*Figure 6: Import Path Applicability Rules for Package Dialog Box*

This enables you to target specific file paths or to include file paths discovered in other partitions in order to create a single patch for deployment that covers all desired file paths.

**CSV File Format**

When creating a CSV file for import, file paths entered in the following formats are acceptable:

```
C:\Users\Administrator\AppData\Local\Temp\Acme\acinstall\tools\acmeinstall\tools\7z.exe
C:\Program Files\Acme\tools\7z.exe
%ProgramFiles%\Acme\tools\7z.exe
```
Note • The CSV file does not need to have comma-separated values, but just a list. You don’t have to use quotes when there are spaces in a file path. The CSV file can essentially be a text list with just one column. As a single column list of values, simply provide one file path per line (no header row or additional columns should be included).

Displaying Latest Microsoft Product Advisory in Smart Groups

Previous versions of Software Vulnerability Manager used to display the most critical advisory applicable for a Microsoft product. This led to situations where very old but critical advisories were shown in the Smart Groups. Since these advisories did not correspond to the latest Knowledge Base articles, they did not give an accurate status in terms of the latest missing Knowledge Base articles for recent “Patch Tuesdays”.

Based on customer feedback, we have tweaked this logic to show the latest advisory instead of the most critical one. This change is in line with patches released on Microsoft’s “Patch Tuesday”, as these patches contain cumulative fixes for older vulnerabilities (CSIL-9669).

Resolved Issues

The following table lists the customer issues that were resolved in Software Vulnerability Manager (On-Premises Edition):

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOJ-2083143</td>
<td>Sorting by criticality column was not working in VPM Grid.</td>
</tr>
<tr>
<td>IOJ-2083144</td>
<td>Sorting by CVSS and CVSS2 columns was not working in product smart groups.</td>
</tr>
<tr>
<td>IOJ-2083662</td>
<td>Numbers next to KB of Windows products does not add up.</td>
</tr>
<tr>
<td>IOJ-2087062</td>
<td>Subscription status incorrect when filtering via smart group.</td>
</tr>
<tr>
<td>IOJ-2096746</td>
<td>VPM packages consuming disk space.</td>
</tr>
<tr>
<td>IOJ-2097405</td>
<td>SVM CentOS VA sending emails with Apache@ email address.</td>
</tr>
<tr>
<td>IOJ-2097487</td>
<td>Products mapped to Rejected Advisories.</td>
</tr>
</tbody>
</table>

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

Copyright © 2020 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/legal/intellectual-property.html. 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.