Introduction

Flexera’s Software Vulnerability Manager 2019 R5 is a Vulnerability and Patch Management Software Solution that facilitates a customized Patch Management process. It combines Vulnerability Intelligence, Threat 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 2019 R5, IT Operations and Security Teams are empowered to prevent vulnerability threats from both Microsoft and non-Microsoft (third-party) product vulnerabilities, covering Microsoft Windows, Mac OS, and Red Hat Enterprise Linux.

Software Vulnerability Manager 2019 R5 integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager.

New Features and Enhancements

Software Vulnerability Manager 2019 R5 On-Premises Edition includes the following new features and enhancements:

- **Vendor Patch Module - Automation**
- **Software Vulnerability Manager Client ToolKit**
- **Mac Agent Support**
- **Ability to Set Maximum Post Data Size**
- **CVE Search in Advisory Smart Groups**
- **CVE Number as Criteria in Host Smart Groups**
- **Extended Support in Non IE Browser**
- **View Installations and Patch Information**
- **Vendor Patch Module - Configure View Enhanced**
- **Timestamping Services - DigiCert**

*Note* To see the following new features and enhancements in your Software Vulnerability Manager 2019 R5 interface, you must refresh your browser’s cache (press Ctrl+F5).

Vendor Patch Module - Automation

With this release of Software Vulnerability Manager 2019, users can automate deployment of patches supported by Vendor Patch Module. The new option **Subscribe to Package** has been added to right click menu. Subscribed packages will be deployed automatically to configured WSUS using a new tool called **Flexera SVM Patch Configuration**, see **Software Vulnerability Manager Client ToolKit**.

*Note* To utilize the Vendor Patch Module - Automation, note the following:

- **Vendor Patch Module is an optional feature and must be purchased separately.**
- **Install the Software Vulnerability Manager Client ToolKit.**

To use this option, navigate to **Patching >> Vendor Patch Module**. List of patches appears, you can know a patch whether it is already subscribed and its status in the **Subscribed** and **Subscription Status** column.
Right click on a patch which you want to subscribe, select the option **Subscribe to Package**.

**Configure Subscription** dialog pane appears, you can choose your preferences from the below options:

Either one of the below preferences must be defined:

- **Always publish a new patch when a new version is available** - Publishes when new version of the patch is available.

- **Only publish a new patch when any of the following are true**: Publishes when any one of the defined preferences are met. To know more about the below preferences, see Appendix B - About Secunia Advisories.

- **SAID CVSS3 score is greater than**
• Criticality is greater than
  • Extremely Critical
  • Highly Critical
  • Moderately Critical
  • Less Critical
  • Not Critical

• Threat score is greater than

• Patched version greater than - By default, current version of a patch will be displayed.

Either one of these options must be selected to define the deployment schedule based on above preferences:

• Trigger subscription rule above now for the current version - Publishes the package right away.
• Trigger subscription rule above next time a new version is available - Start publishes the package when newer version is available.

Software Vulnerability Manager Client ToolKit

In addition to the SVM Multi-Partition Reporting Tool introduced earlier this year, to ease patch automation and WSUS management two tools have been newly added to the Software Vulnerability Manager Client ToolKit.

On successful installation of Software Vulnerability Manager Client ToolKit, below tools will get install and their respective shortcuts will be created in your desktop.

• Flexera SVM Patch Configuration
• Flexera WSUS Management Tool

Prerequisites

The below prerequisites are required:

• .Net Framework 4.6.1 and above.
• OS Requirements:
  • Install Software Vulnerability Manager Client ToolKit in Windows Server 2012 or Windows 8, for Windows 2012 WSUS.
  • Install Software Vulnerability Manager Client ToolKit in Windows Server 2016 or Windows 10, for Windows 2016 WSUS.
  • Install both the Software Vulnerability Manager Patch Configuration and WSUS in the same domain.

Important • You must install Software Vulnerability Manager Patch Client ToolKit to utilize the Vendor Patch Module - Automation. To download this ToolKit, click here.
Flexera SVM Patch Configuration

Flexera SVM Patch Configuration integrates Software Vulnerability Manager application with the configured WSUS server to achieve the automation for subscribed packages.

Flexera SVM Patch Configuration, has three tabs:

- **WSUS Connection**
- **SVM Connection**
- **General**

**WSUS Connection**

WSUS Connection tab prompts you to enter WSUS server credentials and helps you to select computer groups which you want to deploy the packages.

**SVM Connection**

SVM Connection tab prompts you to enter SVM credentials and token will be generated on successful connection.
General

In general tab, you can define the folder path for log files and log level need to be captured. You can set the frequencies to trigger the polling in Check-In Settings.

Flexera WSUS Management Tool

Flexera WSUS Management Tool allows you to manage the packages and configuration settings of WSUS.

This Tool consist of below tabs:

- Patching Information
Patching Information

Patching Information tab prompts you to connect to the WSUS server to view the packages, based on the selected filter option, either 3rd party, Microsoft updates, or both. It also allows you to approve, delete, decline the selected patches and select a computer groups where you want to deploy these approved patches, at the set deadline.

It consist of three sections:

- Filter Update List
- Group Approvals
- Set Approval Deadline

Configuration

In Configuration tab, you can perform the below WSUS configuration actions:

- Test WSUS
- Test GPO Settings
- Generate New Signing Certificate
- Install Signing Certificate
- Export Signing Certificate from WSUS
- Delete Signing Certificate in WSUS
- Create / Update SVM Group Policy Settings
- Dump All GPO Informations
Mac Agent Support

In Software Vulnerability Manager 2019 R5, signed Mac agent has been enhanced to support the newly introduced MacOS Catalina.

Ability to Set Maximum Post Data Size

In Software Vulnerability Manager 2019 R5, you can set a maximum data size posted to the server. By default, the maximum data size is 10MB.

To set a maximum data size:

- **For Agent** - Use the command line `csia.exe -i -L --postdata-maxsize 15 -v -v -v -v > _install.log` during installation.
- **For Manual Scanning** - Use the command line `csia.exe -c --postdata-maxsize 15 -v -v -v -v > _scan.log` during scanning.
- **For Daemon** - In the `HKEY_CURRENT_USER\Software\Secunia\Daemon` registry location, add a PostDataMaxSize key.
- **For Plug-In** - In the `HKEY_CURRENT_USER\Software\Secunia\CSI plugin` registry location, add a PostDataMaxSize key.
CVE Search in Advisory Smart Groups

In Software Vulnerability Manager 2019 R4, you can now search for an advisory using CVE.

To see the list of all advisories, select the **Results >> Advisory Smart Groups >> Configured Advisory Groups >> All Advisories**.

In the **Search** box, enter the **CVE** to search for an Advisory from the **All Advisories** list.

CVE Number as Criteria in Host Smart Groups

In Software Vulnerability Manager 2019, you can add CVE Number as a separate criteria while configuring New Host Smart Group:

To create a New Host Smart Groups, select the **Results >> Host Smart Groups >> Overview & Configuration**.

List of existing smart group appears.

Click **Create New Smart Group** button. **Configure New smart Group wizard** appears.

In the **Criteria** section, you can add CVE Number as shown below:
Extended Support in Non IE Browser

In Software Vulnerability Manager 2019, list of products available in Flexera Package System (SPS) and Patch Template can also be seen in non IE browsers.

After successful login to the Software Vulnerability Manager 2019 in non IE browser (Chrome, Mozilla, etc.), Open Patching, below sections are now available in non IE browsers:

- Flexera Package System (SPS)
- Patch Template

Note • When you right click on a product or patch template in any non IE browser, you will get the below error message.

View Installations and Patch Information

In Software Vulnerability Manager 2019 R5, View Installations and Patch Information of any products in the Vendor Patch Module can also be seen in non IE browsers.

After successful login to the Software Vulnerability Manager 2019 (On-Prem Edition) in non IE browser (Chrome, Mozilla, etc.), Open Patching > Vendor Patch Module, you can see the list of products.

Right click a product, you can see the following options:

- Create an Update Package
- View Installations
- Patch Information
Now you can select the View Installations and the Patch Information details of a product in any browser.

**Note** • Note the below following:

- When you select the Create an Update Package option in non IE browser, you will get the below error message.

![Browser Not Compatible](image)

- To learn more about the Vendor Patch Module, [click here.](#)
- To learn more about creating patches using the Vendor Patch Module, [click here.](#)

**Vendor Patch Module - Configure View Enhanced**

In Software Vulnerability Manager 2019 R5, Configure View of the Vendor Patch Module is enhanced with the below filter options:

- The new drop down **Show** is added along with the **Add more filters** check boxes, you can filter using one of the following option from the drop down:
  - All available Vendor Patches
  - Only those Detected in my environment
  - Only those Not detected in my environment
Timestamping Services - DigiCert

In Software Vulnerability Manager 2019 R5, Flexera SPS Timestamp url has been changed to support DigiCert Timestamp provider. This was done in reaction to VeriSign and Symantec Timestamping services moving to DigiCert.com as mentioned in https://knowledge.digicert.com/alerts/migration-of-legacy-verisign-and-symantec-time-stamping-services.html.

In Configuration > Settings > Flexera SPS Timestamp, select DigiCert sha256 from the drop down.

Note • TimeStamp Settings can only be set by the Partition Administrator

Resolved Issues

The following table lists the customer issues that were resolved in Software Vulnerability Manager 2019 R5:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOJ-2068477</td>
<td>RHEL 8 Agent Support</td>
</tr>
<tr>
<td>IOJ-2085793</td>
<td>Provide override for agent to post file greater than 10mb</td>
</tr>
<tr>
<td>IOJ-1992395</td>
<td>Unexpected Error after editing the smart groups</td>
</tr>
</tbody>
</table>
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 online community at https://flexeracommunity.force.com/customer/ideas/ideaList.apexp.

System Requirements

To use the Software Vulnerability Manager 2019 R5 console, your system should meet the following requirements:

- Minimum resolution: 1280x1024
- Internet Explorer 11 or higher (Scan results can also be viewed from other browsers)
- Internet connection capable of connecting to https://csi7.secunia.com
- The following addresses should be white-listed in the Firewall/Proxy configuration:
  - crl.verisign.net
  - crl.thawte.com
  - http://crl3.digicert.com
  - http://crl4.digicert.com
  - http://*.ws.symantec.com
  - https://*.secunia.com/
  - http://*.symcb.com
  - http://*.symcd.com
- First-Party cookie settings at least to Prompt (in Internet Explorer)
- Allow session cookies
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.