Software Vulnerability Manager 2019 R5 On-Premises Edition
Release Notes

December 2019

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

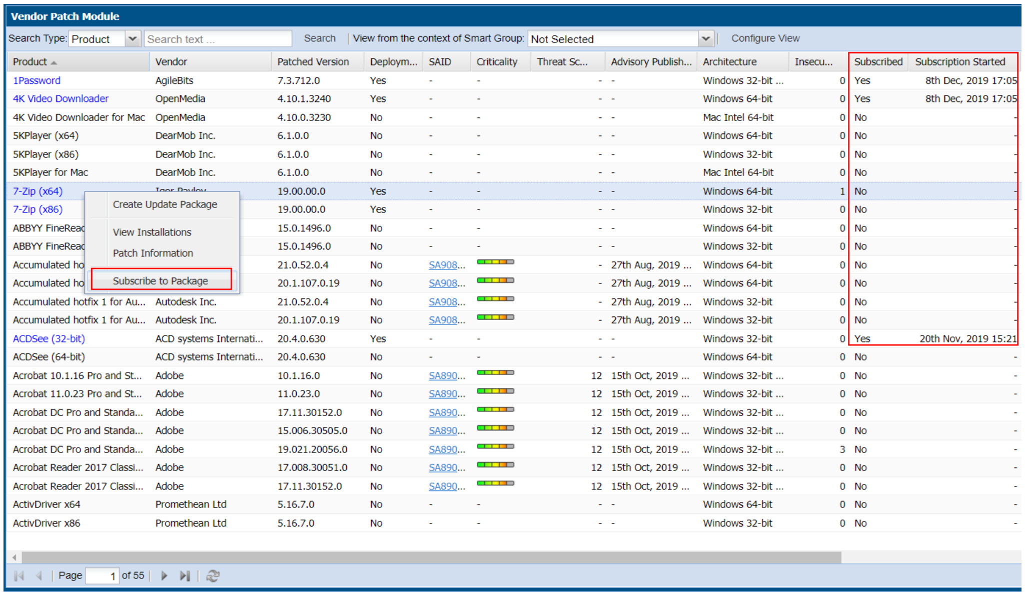
With this release of Software Vulnerability Manager 2019, users can automate deployment of patches supported by Vendor Patch Module. The new option **Subscribe to Package** has been added to right click menu. Subscribed packages will be deployed automatically to configured WSUS using a new tool called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



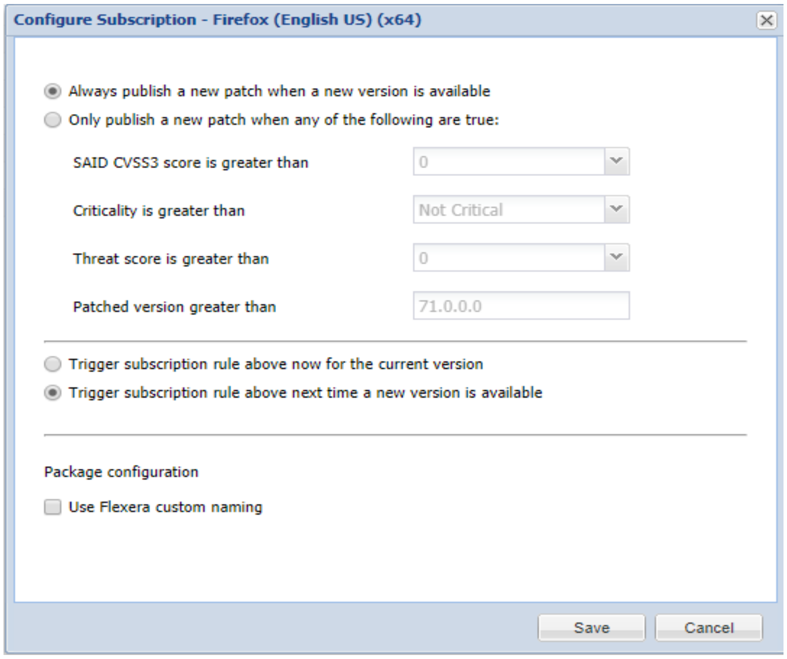
Vendor Patch Module

Search Type: Product | Search text ... | Search | View from the context of Smart Group: Not Selected | Configure View

Product	Vendor	Patched Version	Deploym...	SAID	Criticality	Threat Sc...	Advisory Publish...	Architecture	Insecu...	Subscribed	Subscription Started
1Password	AgileBits	7.3.712.0	Yes	-	-	-	-	Windows 32-bit ...	0	Yes	8th Dec, 2019 17:05
4K Video Downloader	OpenMedia	4.10.1.3240	Yes	-	-	-	-	Windows 64-bit	0	Yes	8th Dec, 2019 17:05
4K Video Downloader for Mac	OpenMedia	4.10.0.3230	No	-	-	-	-	Mac Intel 64-bit	0	No	-
5KPlayer (x64)	DearMob Inc.	6.1.0.0	No	-	-	-	-	Windows 64-bit	0	No	-
5KPlayer (x86)	DearMob Inc.	6.1.0.0	No	-	-	-	-	Windows 32-bit	0	No	-
5KPlayer for Mac	DearMob Inc.	6.1.0.0	No	-	-	-	-	Mac Intel 64-bit	0	No	-
7-Zip (x64)	Igor Pavlov	19.00.00.0	Yes	-	-	-	-	Windows 64-bit	1	No	-
7-Zip (x86)		19.00.00.0	Yes	-	-	-	-	Windows 32-bit	0	No	-
ABBYY FineReac		15.0.1496.0	No	-	-	-	-	Windows 64-bit	0	No	-
ABBYY FineReac		15.0.1496.0	No	-	-	-	-	Windows 32-bit	0	No	-
Accumulated ho		21.0.52.0.4	No	SA908...	▰▰▰▰▱	-	27th Aug, 2019 ...	Windows 64-bit	0	No	-
Accumulated ho		20.1.107.0.19	No	SA908...	▰▰▰▰▱	-	27th Aug, 2019 ...	Windows 64-bit	0	No	-
Accumulated hotfix 1 for Au...	Autodesk Inc.	21.0.52.0.4	No	SA908...	▰▰▰▰▱	-	27th Aug, 2019 ...	Windows 32-bit	0	No	-
Accumulated hotfix 1 for Au...	Autodesk Inc.	20.1.107.0.19	No	SA908...	▰▰▰▰▱	-	27th Aug, 2019 ...	Windows 32-bit	0	No	-
ACDSee (32-bit)	ACD systems Internati...	20.4.0.630	Yes	-	-	-	-	Windows 32-bit	0	Yes	20th Nov, 2019 15:21
ACDSee (64-bit)	ACD systems Internati...	20.4.0.630	No	-	-	-	-	Windows 64-bit	0	No	-
Acrobat 10.1.16 Pro and St...	Adobe	10.1.16.0	No	SA890...	▰▰▰▰▱	12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	-
Acrobat 11.0.23 Pro and St...	Adobe	11.0.23.0	No	SA890...	▰▰▰▰▱	12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	-
Acrobat DC Pro and Standa...	Adobe	17.11.30152.0	No	SA890...	▰▰▰▰▱	12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	-
Acrobat DC Pro and Standa...	Adobe	15.006.30505.0	No	SA890...	▰▰▰▰▱	12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	-
Acrobat DC Pro and Standa...	Adobe	19.021.20056.0	No	SA890...	▰▰▰▰▱	12	15th Oct, 2019 ...	Windows 32-bit ...	3	No	-
Acrobat Reader 2017 Classi...	Adobe	17.008.30051.0	No	SA890...	▰▰▰▰▱	12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	-
Acrobat Reader 2017 Classi...	Adobe	17.11.30152.0	No	SA890...	▰▰▰▰▱	12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	-
ActivDriver x64	Promethean Ltd	5.16.7.0	No	-	-	-	-	Windows 64-bit	0	No	-
ActivDriver x86	Promethean Ltd	5.16.7.0	No	-	-	-	-	Windows 32-bit	0	No	-

Page 1 of 55

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



Configure Subscription - Firefox (English US) (x64)

● Always publish a new patch when a new version is available

○ Only publish a new patch when any of the following are true:

SAID CVSS3 score is greater than: 0

Criticality is greater than: Not Critical

Threat score is greater than: 0

Patched version greater than: 71.0.0.0

○ Trigger subscription rule above now for the current version

● Trigger subscription rule above next time a new version is available

Package configuration

□ Use Flexera custom naming

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 option 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

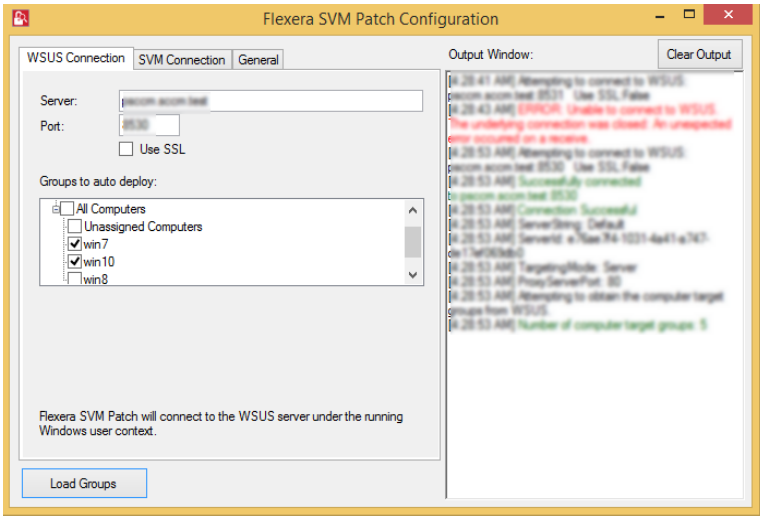
Flexera SVM Patch Configuration integrates Software Vulnerability Manager application with the configured WSUS server to achieve the automation for subscribed packages.

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.



Server: [illegible]

Port: [illegible]

☐ Use SSL

Groups to auto deploy:

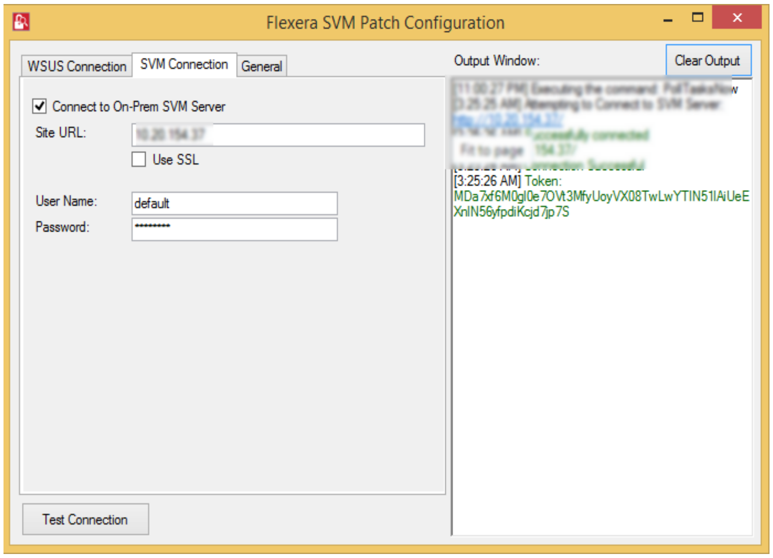
- ☐ All Computers
  - ☐ Unassigned Computers
  - ☑ win7
  - ☑ win10
  - ☐ win8

Flexera SVM Patch will connect to the WSUS server under the running Windows user context.

```
[4:28:41 AM] Attempting to connect to WSUS:
[illegible]:8531   Use SSL False
[4:28:43 AM] ERROR: Unable to connect to WSUS.
The underlying connection was closed: An unexpected
error occurred on a receive.
[4:28:53 AM] Attempting to connect to WSUS:
[illegible]:8530   Use SSL False
[4:28:53 AM] Successfully connected
to [illegible]:8530
[4:28:53 AM] Connection Successful
[4:28:53 AM] ServerString: Default
[4:28:53 AM] ServerId: [illegible]
[4:28:53 AM] TargetingMode: Server
[4:28:53 AM] ProxyServerPort: 80
[4:28:53 AM] Attempting to obtain the computer target
groups from WSUS.
[4:28:53 AM] Number of computer target groups: 5
```

SVM Connection

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



☑ Connect to On-Prem SVM Server

Site URL: [illegible]

☐ Use SSL

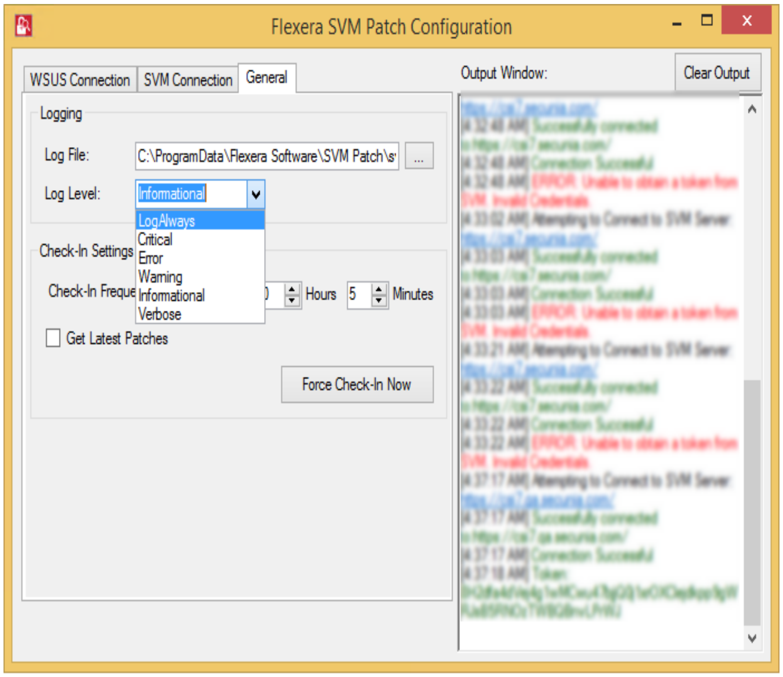
User Name: default

Password: ********

```
[3:25:26 AM] Token:
MDa7xf6M0gl0e7OVt3MfyUoyVX08TwLwYTIN51lAiUeE
XnlN56yfpdiKcjd7jp7S
```

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.



Log File: C:\ProgramData\Flexera Software\SVM Patch\s

Log Level: Informational

Check-In Freque… Hours 5 Minutes

☐ Get Latest Patches

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

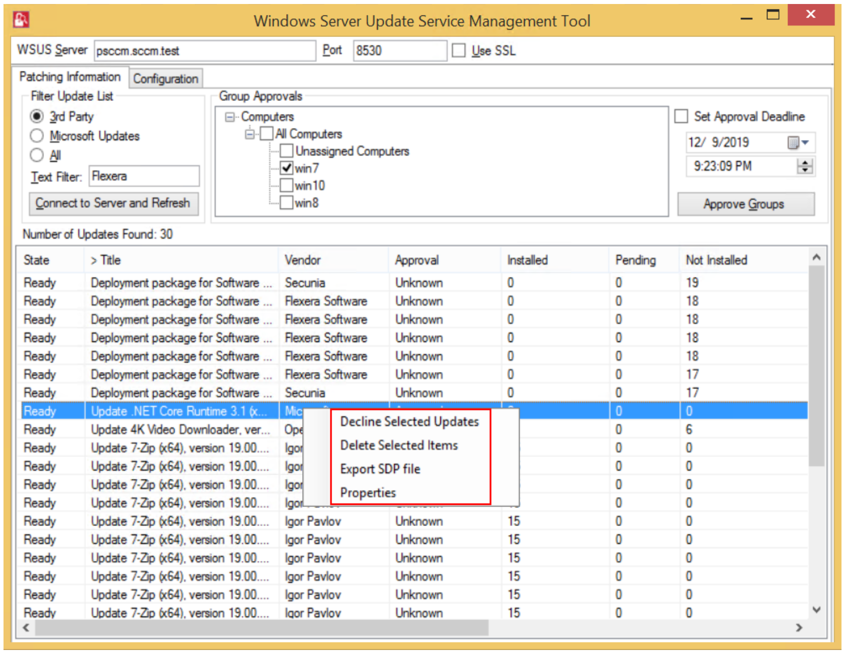
- Configuration

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



Windows Server Update Service Management Tool

WSUS Server: psccm.sccm.test Port: 8530 □ Use SSL

Patching Information | Configuration

Filter Update List
- ● 3rd Party
- ○ Microsoft Updates
- ○ All

Text Filter: Flexera

Connect to Server and Refresh

Group Approvals
- Computers
  - □ All Computers
    - □ Unassigned Computers
    - ☑ win7
    - □ win10
    - □ win8

□ Set Approval Deadline

12/ 9/2019

9:23:09 PM

Approve Groups

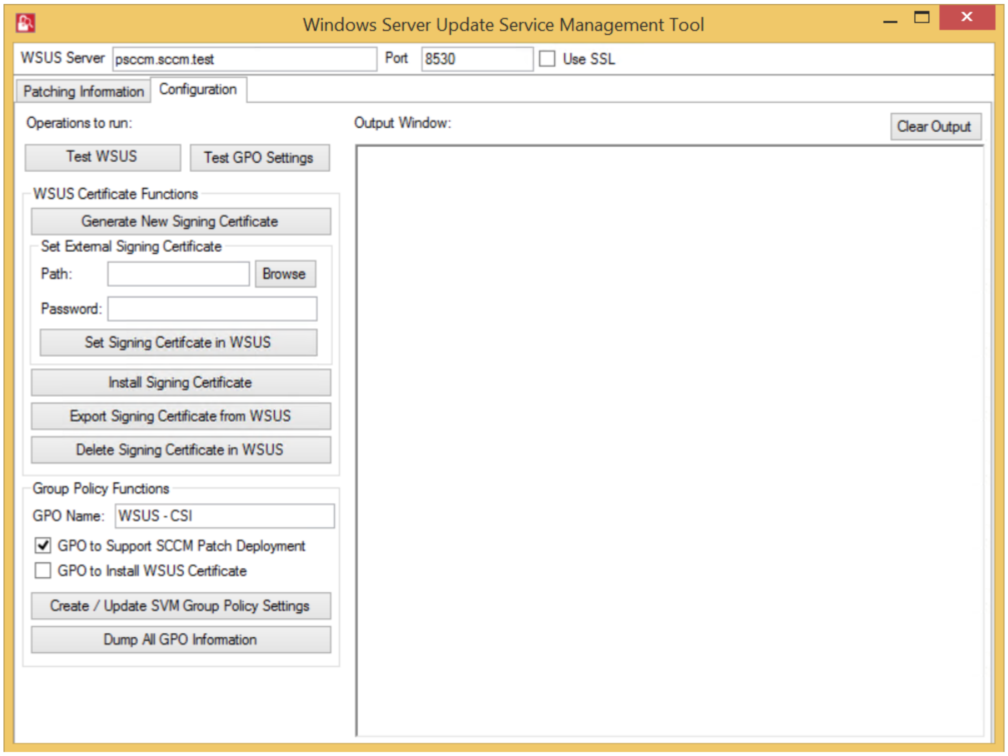
Number of Updates Found: 30

State	> Title	Vendor	Approval	Installed	Pending	Not Installed
Ready	Deployment package for Software ...	Secunia	Unknown	0	0	19
Ready	Deployment package for Software ...	Flexera Software	Unknown	0	0	18
Ready	Deployment package for Software ...	Flexera Software	Unknown	0	0	18
Ready	Deployment package for Software ...	Flexera Software	Unknown	0	0	18
Ready	Deployment package for Software ...	Flexera Software	Unknown	0	0	18
Ready	Deployment package for Software ...	Flexera Software	Unknown	0	0	17
Ready	Deployment package for Software ...	Secunia	Unknown	0	0	17
Ready	Update .NET Core Runtime 3.1 (x...	Mic			0	0
Ready	Update 4K Video Downloader, ver...	Ope			0	6
Ready	Update 7-Zip (x64), version 19.00....	Igor			0	0
Ready	Update 7-Zip (x64), version 19.00....	Igor			0	0
Ready	Update 7-Zip (x64), version 19.00....	Igor			0	0
Ready	Update 7-Zip (x64), version 19.00....	Igor			0	0
Ready	Update 7-Zip (x64), version 19.00....	Igor Pavlov	Unknown	15	0	0
Ready	Update 7-Zip (x64), version 19.00....	Igor Pavlov	Unknown	15	0	0
Ready	Update 7-Zip (x64), version 19.00....	Igor Pavlov	Unknown	15	0	0
Ready	Update 7-Zip (x64), version 19.00....	Igor Pavlov	Unknown	15	0	0
Ready	Update 7-Zip (x64), version 19.00....	Igor Pavlov	Unknown	15	0	0
Ready	Update 7-Zip (x64), version 19.00....	Igor Pavlov	Unknown	15	0	0

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



Windows Server Update Service Management Tool
Patching Information
Configuration
Operations to run:
Test WSUS
Test GPO Settings
WSUS Certificate Functions
Generate New Signing Certificate
Set External Signing Certificate
Path:
Browse
Password:
Set Signing Certifcate in WSUS
Install Signing Certificate
Export Signing Certificate from WSUS
Delete Signing Certificate in WSUS
Group Policy Functions
Create / Update SVM Group Policy Settings
Dump All GPO Information
Output Window:
Clear Output

WSUS Server psccm.sccm.test Port 8530 ☐ Use SSL

GPO Name: WSUS - CSI

☑ GPO to Support SCCM Patch Deployment

☐ GPO to Install WSUS Certificate

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:

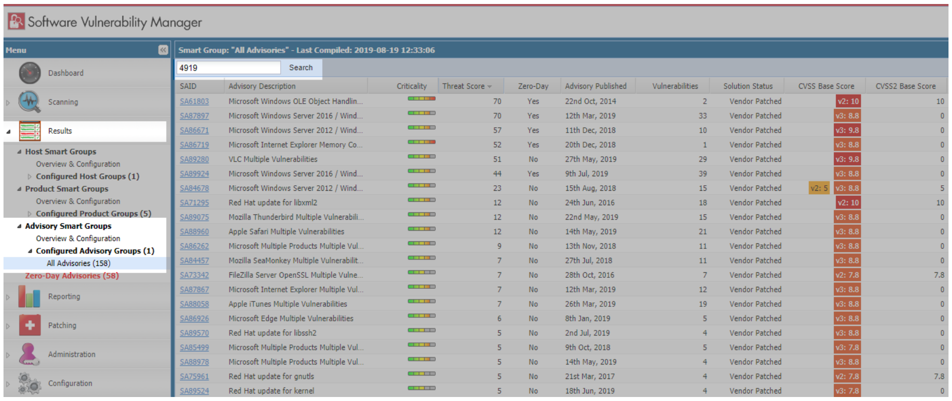
- **For Agent** - Use the command line **csia.exe -i -L --postdata-maxsize 15 -v -v -v -v > _install.log** during installation.
- **For Manual Scanning** - Use the command line **csia.exe -c --postdata-maxsize 15 -v -v -v -v > _scan.log** during scanning.
- **For Daemon** - In the **HKEY_CURRENT_USER\Software\Secunia\Daemon** 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.



Smart Group: "All Advisories" - Last Compiled: 2019-08-19 12:33:06

4919

SAID	Advisory Description	Criticality	Threat Score	Zero-Day	Advisory Published	Vulnerabilities	Solution Status	CVSS Base Score	CVSS2 Base Score
SA61803	Microsoft Windows OLE Object Handlin...		70	Yes	22nd Oct, 2014	2	Vendor Patched	v2: 10	10
SA87897	Microsoft Windows Server 2016 / Wind...		70	Yes	12th Mar, 2019	33	Vendor Patched	v3: 8.8	0
SA86671	Microsoft Windows Server 2012 / Wind...		57	Yes	11th Dec, 2018	10	Vendor Patched	v3: 9.8	0
SA86719	Microsoft Internet Explorer Memory Co...		52	Yes	20th Dec, 2018	1	Vendor Patched	v3: 8.8	0
SA89280	VLC Multiple Vulnerabilities		51	No	27th May, 2019	29	Vendor Patched	v3: 9.8	0
SA89924	Microsoft Windows Server 2016 / Wind...		44	Yes	9th Jul, 2019	39	Vendor Patched	v3: 8.8	0
SA84678	Microsoft Windows Server 2012 / Wind...		23	No	15th Aug, 2018	15	Vendor Patched	v2: 5 v3: 8.8	5
SA71295	Red Hat update for libxml2		12	No	24th Jun, 2016	18	Vendor Patched	v2: 10	10
SA89075	Mozilla Thunderbird Multiple Vulnerabili...		12	No	22nd May, 2019	15	Vendor Patched	v3: 8.8	0
SA88960	Apple Safari Multiple Vulnerabilities		12	No	14th May, 2019	21	Vendor Patched	v3: 8.8	0
SA86262	Microsoft Multiple Products Multiple Vul...		9	No	13th Nov, 2018	11	Vendor Patched	v3: 8.8	0
SA84457	Mozilla SeaMonkey Multiple Vulnerabilit...		7	No	27th Jul, 2018	11	Vendor Patched	v3: 8.8	0
SA73342	FileZilla Server OpenSSL Multiple Vulne...		7	No	28th Oct, 2016	7	Vendor Patched	v2: 7.8	7.8
SA87867	Microsoft Internet Explorer Multiple Vul...		7	No	12th Mar, 2019	12	Vendor Patched	v3: 8.8	0
SA88058	Apple iTunes Multiple Vulnerabilities		7	No	26th Mar, 2019	19	Vendor Patched	v3: 8.8	0
SA86926	Microsoft Edge Multiple Vulnerabilities		6	No	8th Jan, 2019	5	Vendor Patched	v3: 8.8	0
SA89570	Red Hat update for libssh2		5	No	2nd Jul, 2019	4	Vendor Patched	v3: 8.8	0
SA85499	Microsoft Multiple Products Multiple Vul...		5	No	9th Oct, 2018	5	Vendor Patched	v3: 7.8	0
SA88978	Microsoft Multiple Products Multiple Vul...		5	No	14th May, 2019	4	Vendor Patched	v3: 8.8	0
SA75961	Red Hat update for gnutls		5	No	21st Mar, 2017	4	Vendor Patched	v2: 7.8	7.8
SA89524	Red Hat update for kernel		5	No	18th Jun, 2019	4	Vendor Patched	v3: 7.8	0

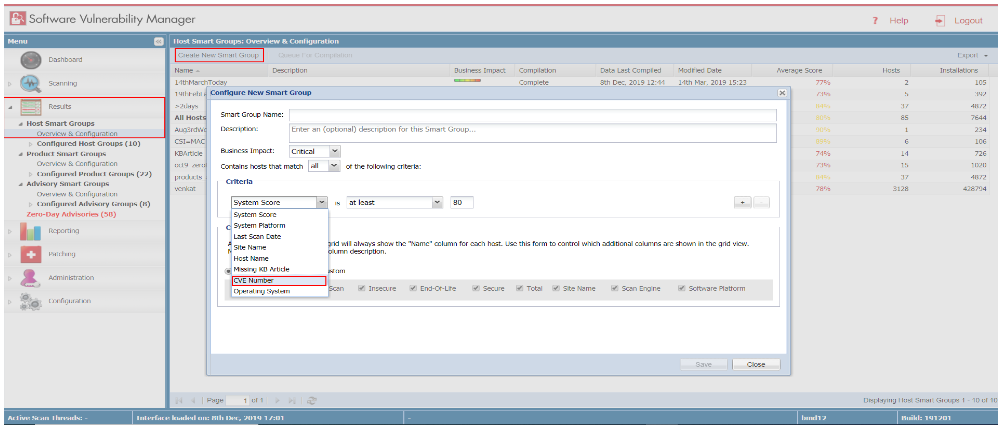
CVE Number as Criteria in Host Smart Groups

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:



Host Smart Groups: Overview & Configuration

Name	Description	Business Impact	Compilation	Data Last Compiled	Modified Date	Average Score	Hosts	Installations
14thMarchToday			Complete	8th Dec, 2019 12:44	14th Mar, 2019 15:23	77%	2	105
19thFebLa						73%	5	392
>2days						84%	37	4872
All Hosts						80%	85	7644
Aug3rdWe						90%	1	234
CSI=MAC						89%	6	106
KBArticle						74%	14	726
oct9_zerol						73%	15	1020
products_						84%	37	4872
venkat						78%	3128	428794

Configure New Smart Group

Smart Group Name:

Description: Enter an (optional) description for this Smart Group...

Business Impact: Critical

Contains hosts that match all of the following criteria:

Criteria

System Score is at least 80

A... grid will always show the "Name" column for each host. Use this form to control which additional columns are shown in the grid view. M... olumn description.

● ...ustom

...Scan ☑ Insecure ☑ End-Of-Life ☑ Secure ☑ Total ☑ Site Name ☑ Scan Engine ☑ Software Platform

Page 1 of 1

Displaying Host Smart Groups 1 - 10 of 10

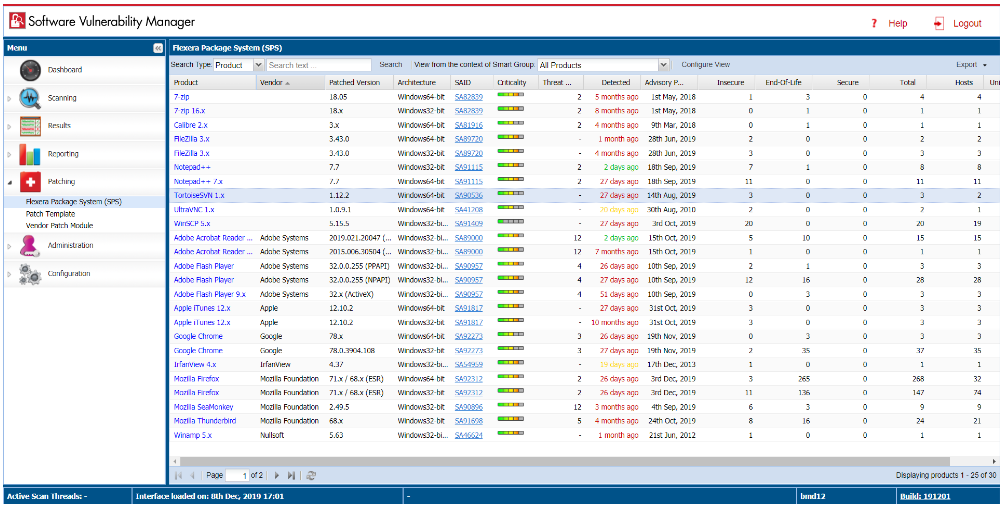
Active Scan Threads: - | Interface loaded on: 8th Dec, 2019 17:01 | - | bmd12 | Build: 191201

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



Flexera Package System (SPS)

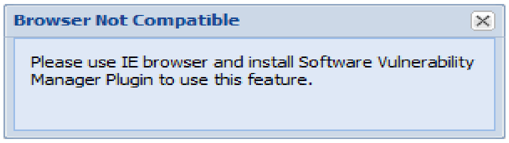
Search Type: Product | Search text ... | Search | View from the context of Smart Group: All Products | Configure View | Export

Product	Vendor	Patched Version	Architecture	SAID	Criticality	Threat ...	Detected	Advisory P...	Insecure	End-Of-Life	Secure	Total	Hosts	Uni
7-zip		18.05	Windows64-bit	SA82839		2	5 months ago	1st May, 2018	1	3	0	4	4	
7-zip 16.x		18.x	Windows32-bit	SA82839		2	8 months ago	1st May, 2018	0	1	0	1	1	
Calibre 2.x		3.x	Windows64-bit	SA81916		2	4 months ago	9th Mar, 2018	0	1	0	1	1	
FileZilla 3.x		3.43.0	Windows64-bit	SA89720		-	1 month ago	28th Jun, 2019	2	0	0	2	2	
FileZilla 3.x		3.43.0	Windows32-bit	SA89720		-	4 months ago	28th Jun, 2019	3	0	0	3	3	
Notepad++		7.7	Windows32-bit	SA91115		2	2 days ago	18th Sep, 2019	7	1	0	8	8	
Notepad++ 7.x		7.7	Windows64-bit	SA91115		2	27 days ago	18th Sep, 2019	11	0	0	11	11	
TortoiseSVN 1.x		1.12.2	Windows64-bit	SA90536		-	27 days ago	14th Aug, 2019	3	0	0	3	2	
UltraVNC 1.x		1.0.9.1	Windows64-bit	SA41208		-	20 days ago	30th Aug, 2010	2	0	0	2	1	
WinSCP 5.x		5.15.5	Windows32-bi...	SA91409		-	27 days ago	3rd Oct, 2019	20	0	0	20	19	
Adobe Acrobat Reader ...	Adobe Systems	2019.021.20047 (...	Windows32-bi...	SA89000		12	2 days ago	15th Oct, 2019	5	10	0	15	15	
Adobe Acrobat Reader ...	Adobe Systems	2015.006.30504 (...	Windows32-bi...	SA89000		12	7 months ago	15th Oct, 2019	1	0	0	1	1	
Adobe Flash Player	Adobe Systems	32.0.0.255 (PPAPI)	Windows32-bi...	SA90957		4	26 days ago	10th Sep, 2019	2	1	0	3	3	
Adobe Flash Player	Adobe Systems	32.0.0.255 (NPAPI)	Windows32-bi...	SA90957		4	27 days ago	10th Sep, 2019	12	16	0	28	28	
Adobe Flash Player 9.x	Adobe Systems	32.x (ActiveX)	Windows32-bi...	SA90957		4	51 days ago	10th Sep, 2019	0	3	0	3	3	
Apple iTunes 12.x	Apple	12.10.2	Windows64-bit	SA91817		-	27 days ago	31st Oct, 2019	3	0	0	3	3	
Apple iTunes 12.x	Apple	12.10.2	Windows32-bit	SA91817		-	10 months ago	31st Oct, 2019	3	0	0	3	3	
Google Chrome	Google	78.x	Windows64-bit	SA92273		3	26 days ago	19th Nov, 2019	0	3	0	3	3	
Google Chrome	Google	78.0.3904.108	Windows32-bit	SA92273		3	27 days ago	19th Nov, 2019	2	35	0	37	35	
IrfanView 4.x	IrfanView	4.37	Windows32-bi...	SA54959		-	19 days ago	17th Dec, 2013	1	0	0	1	1	
Mozilla Firefox	Mozilla Foundation	71.x / 68.x (ESR)	Windows64-bit	SA92312		2	26 days ago	3rd Dec, 2019	3	265	0	268	32	
Mozilla Firefox	Mozilla Foundation	71.x / 68.x (ESR)	Windows32-bit	SA92312		2	26 days ago	3rd Dec, 2019	11	136	0	147	74	
Mozilla SeaMonkey	Mozilla Foundation	2.49.5	Windows32-bit	SA90896		12	3 months ago	4th Sep, 2019	6	3	0	9	9	
Mozilla Thunderbird	Mozilla Foundation	68.x	Windows32-bit	SA91698		5	4 months ago	24th Oct, 2019	8	16	0	24	21	
Winamp 5.x	Nullsoft	5.63	Windows32-bi...	SA46624		-	1 month ago	21st Jun, 2012	1	0	0	1	1	

Page 1 of 2 | Displaying products 1 - 25 of 30

Active Scan Threads: - | Interface loaded on: 8th Dec, 2019 17:01 | - | bmd12 | Build: 191201

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



Browser Not Compatible

Please use IE browser and install Software Vulnerability Manager Plugin to use this feature.

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.

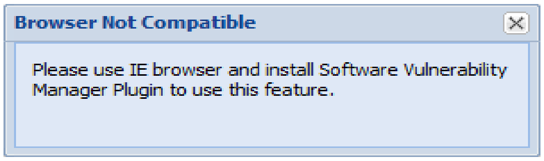
Right click a product, you can see the following options:

- 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

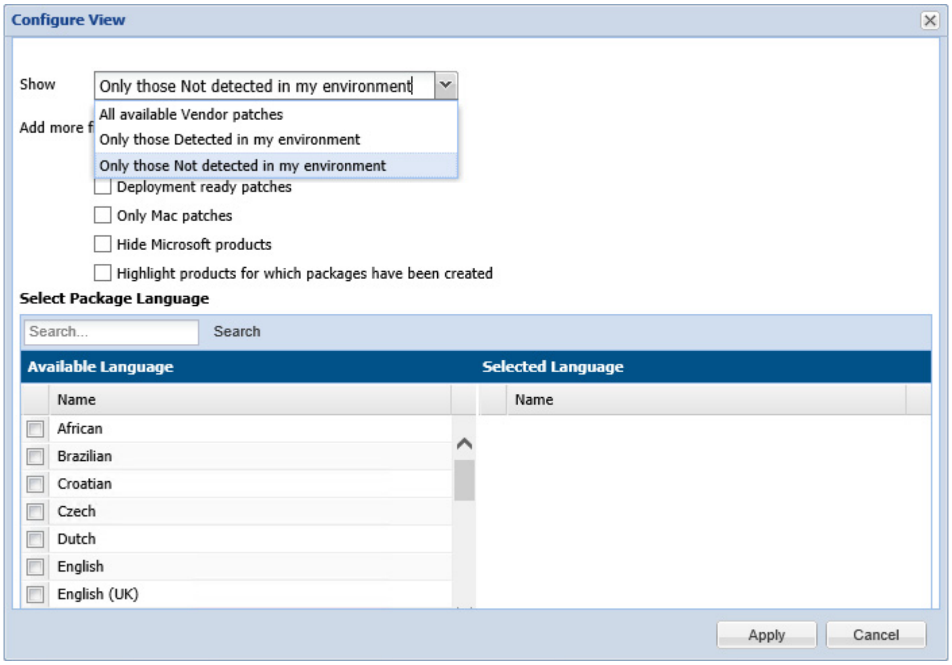
Please use IE browser and install Software Vulnerability Manager Plugin to use this feature.

- *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



Configure View

Show: Only those Not detected in my environment

Add more f

□ Deployment ready patches
□ Only Mac patches
□ Hide Microsoft products
□ Highlight products for which packages have been created

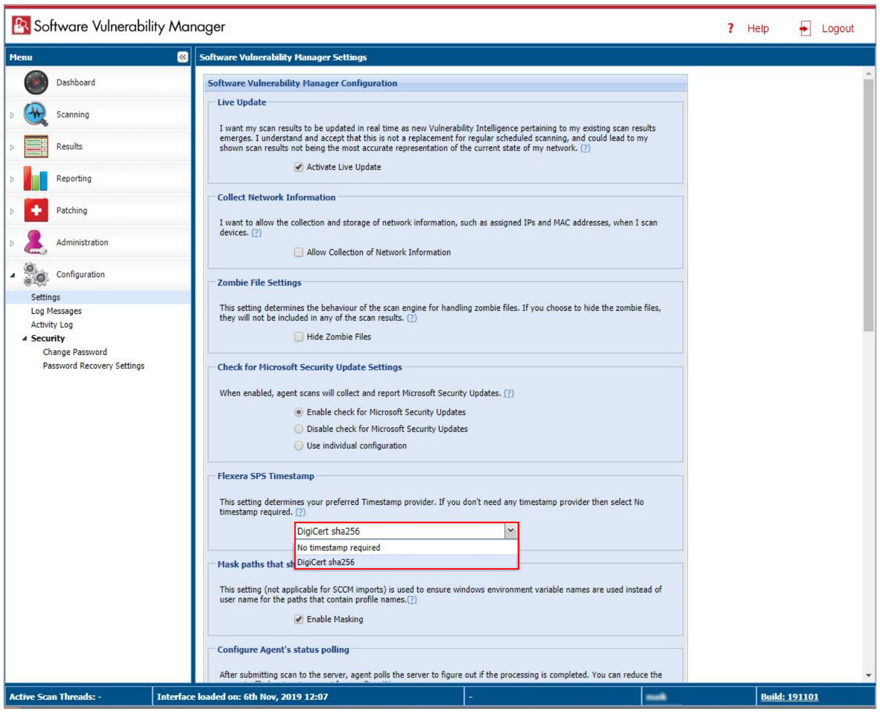
Select Package Language

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*



Software Vulnerability Manager Settings

Software Vulnerability Manager Configuration

Live Update

I want my scan results to be updated in real time as new Vulnerability Intelligence pertaining to my existing scan results emerges. I understand and accept that this is not a replacement for regular scheduled scanning, and could lead to my shown scan results not being the most accurate representation of the current state of my network. (?)

☑ Activate Live Update

Collect Network Information

I want to allow the collection and storage of network information, such as assigned IPs and MAC addresses, when I scan devices. (?)

☐ Allow Collection of Network Information

Zombie File Settings

This setting determines the behaviour of the scan engine for handling zombie files. If you choose to hide the zombie files, they will not be included in any of the scan results. (?)

☐ Hide Zombie Files

Check for Microsoft Security Update Settings

When enabled, agent scans will collect and report Microsoft Security Updates. (?)

● Enable check for Microsoft Security Updates
○ Disable check for Microsoft Security Updates
○ Use individual configuration

Flexera SPS Timestamp

This setting determines your preferred Timestamp provider. If you don't need any timestamp provider then select No timestamp required. (?)

DigiCert sha256
No timestamp required
DigiCert sha256

Mask paths that sh

This setting (not applicable for SCCM imports) is used to ensure windows environment variable names are used instead of user name for the paths that contain profile names.(?)

☑ Enable Masking

Configure Agent's status polling

After submitting scan to the server, agent polls the server to figure out if the processing is completed. You can reduce the

Active Scan Threads: - | Interface loaded on: 6th Nov, 2019 12:07 | - | [redacted] | Build: 191101

Resolved Issues

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

Issue	Description
IOJ-2068477	RHEL 8 Agent Support
IOJ-2085793	Provide override for agent to post file greater than 10mb
IOJ-1992395	Unexpected Error after editing the smart groups

Issue	Description
IOJ-1910914	Some Packages Displayed without a Name in SPS - Cannot Pass After Step 2 in the Wizard
IOJ-1900203	[ActivtyLog] Clearing WUA options does not log into activity log
IOJ-1886345	IP Access Management: Scheduled Export generates an empty CSV file.
IOJ-1990701	When two or more product_ids are associated with the same VPM_id, in the pop window of "view installations" data for all the product_ids is not displaying
IOJ-2079064	Unexpected error while creating a smart group by using a template

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

- A PDF reader

Legal Information

Copyright Notice

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.