Software Vulnerability Manager 2019 (Cloud Edition)
Release Notes

December 2019

Introduction

Flexera's Software Vulnerability Manager 2019 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, 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 integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager.

New Features and Enhancements

Software Vulnerability Manager 2019 (Cloud Edition) includes the following new features and enhancements:

- Vendor Patch Module - Automation
- Software Vulnerability Manager Client ToolKit
- Extended Support in Non IE Browser
- CVE Number as Criteria in Host Smart Groups

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

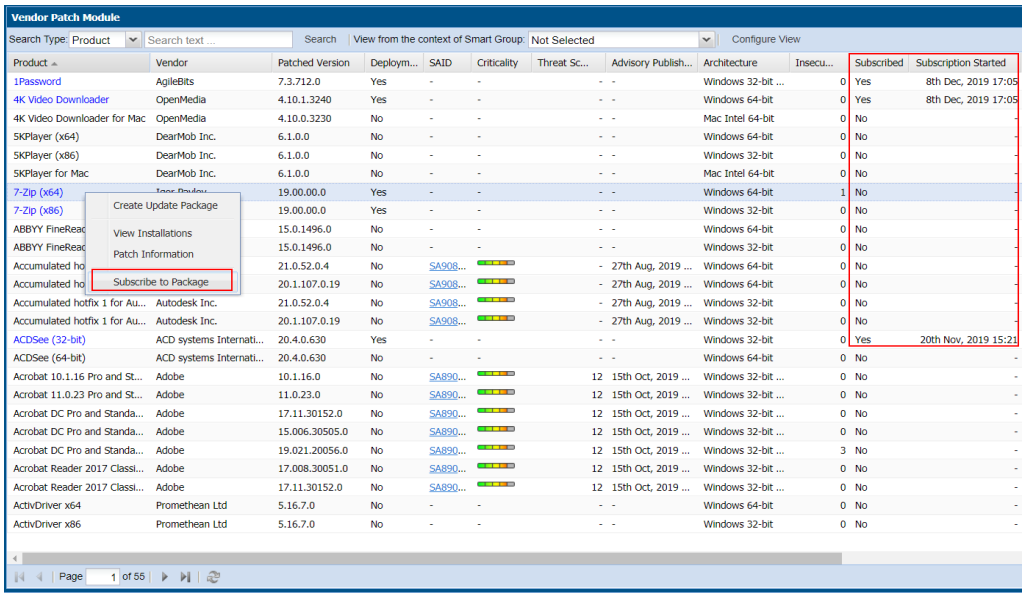
Vendor Patch Module - Automation

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 • *Install Software Vulnerability Manager Client ToolKit to utilize the Vendor Patch Module - Automation.*

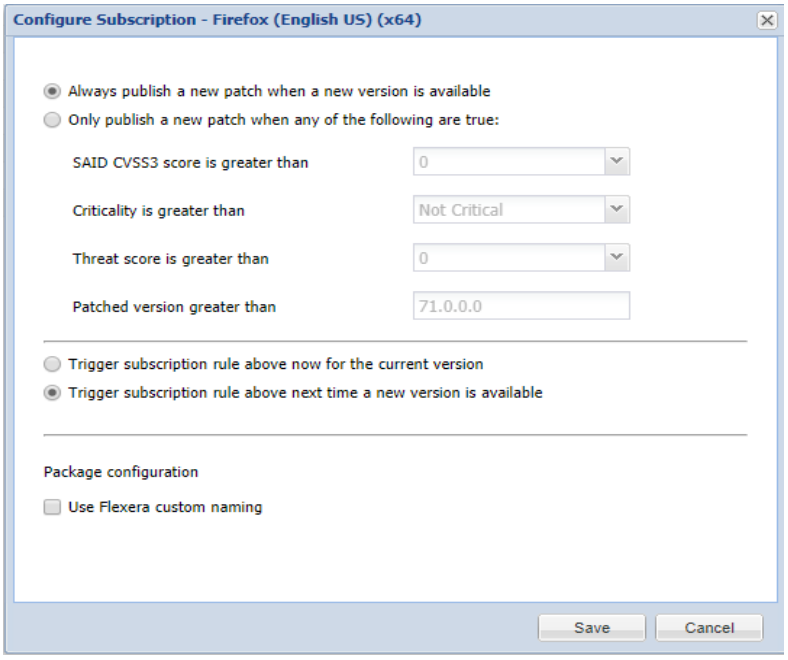
To use this option, navigate to **Patching >> Vendor Patch Module**. List of patches appears, you can know a patch whether it is already subscribed and its status in the **Subscribed** and **Subscription Status** column.

Right click on a patch which you want to subscribe, select the option **Subscribe to Package**.



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)	[illegible]	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	-

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 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

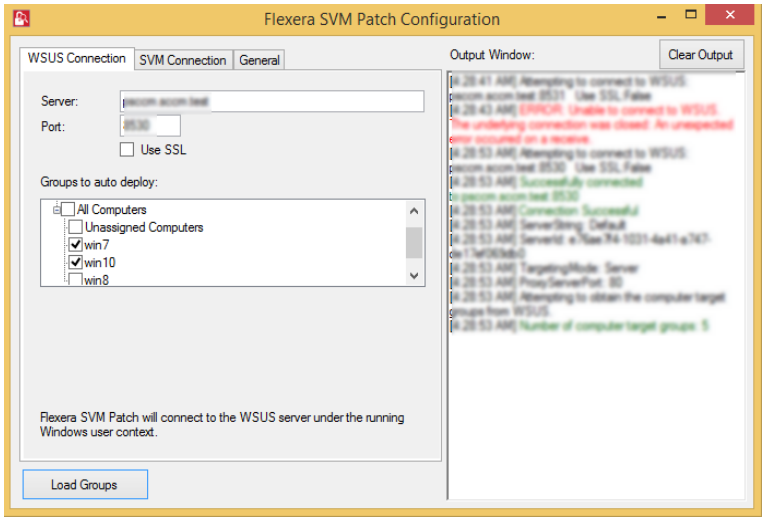
Flexera SVM Patch Configuration integrates Software Vulnerability Manager application with the configured WSUS server to achieve the automation for subscribed packages.

Flexera SVM Patch Configuration, has three tabs:

- WSUS Connection
- SVM Connection
- General

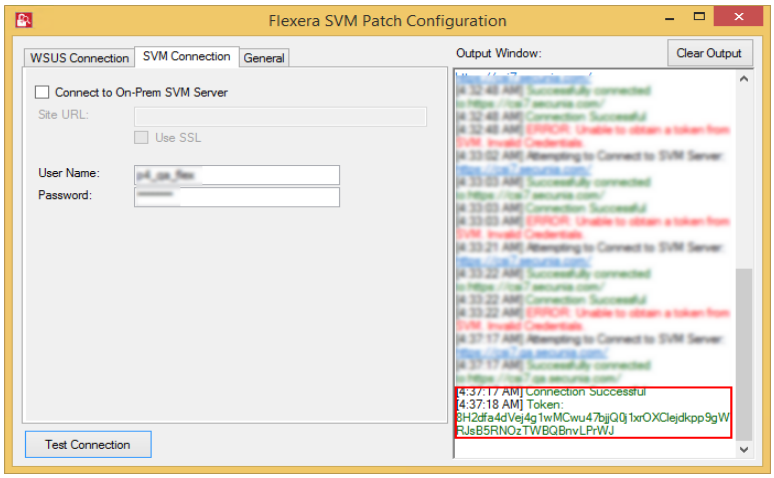
WSUS Connection

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



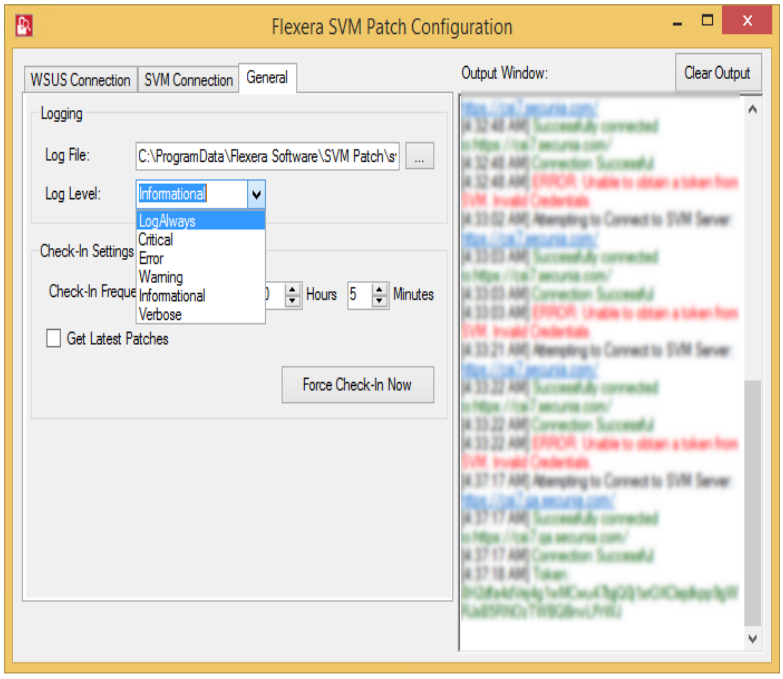
SVM Connection

SVM Connection tab prompts you to enter a 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:

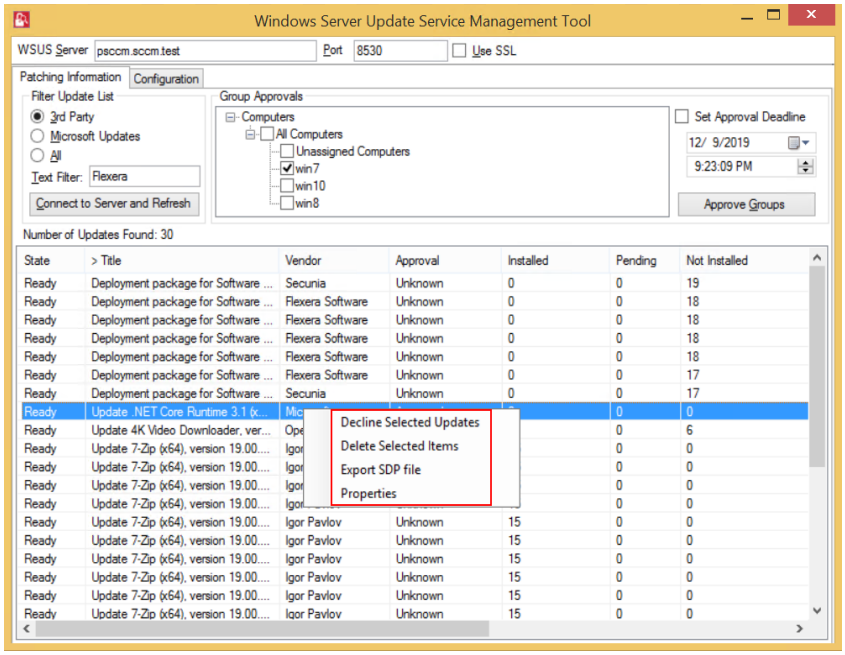
- Patching Information
- Configuration

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:

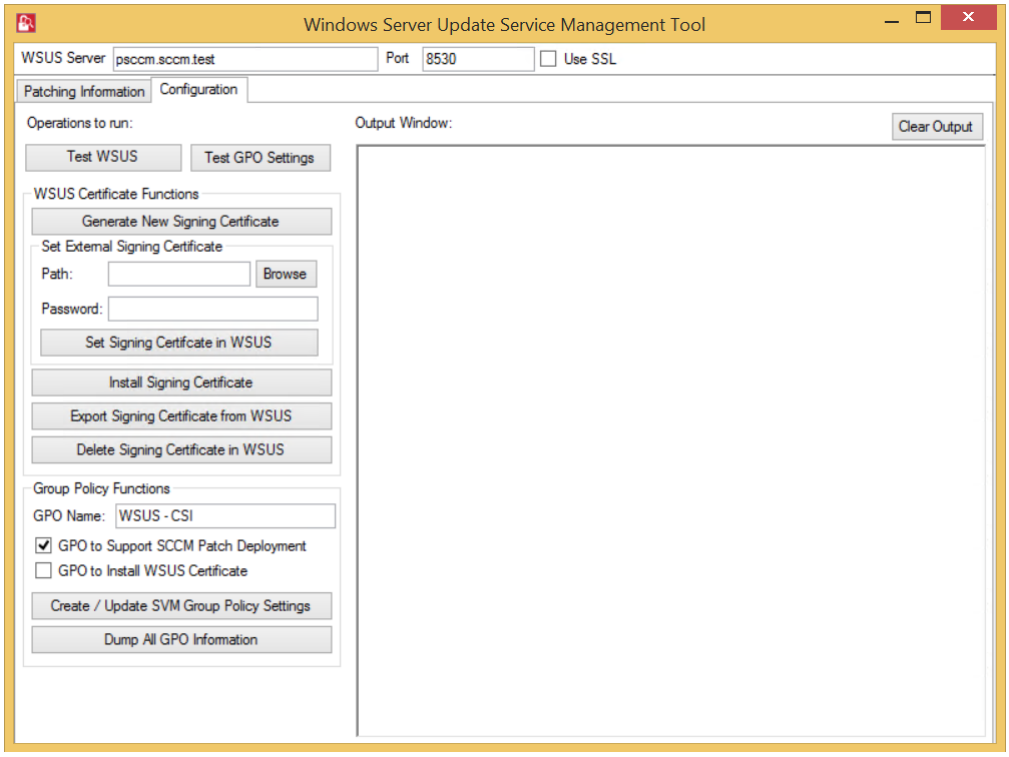
- Filter Update List
- Group Approvals
- Set Approval Deadline



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

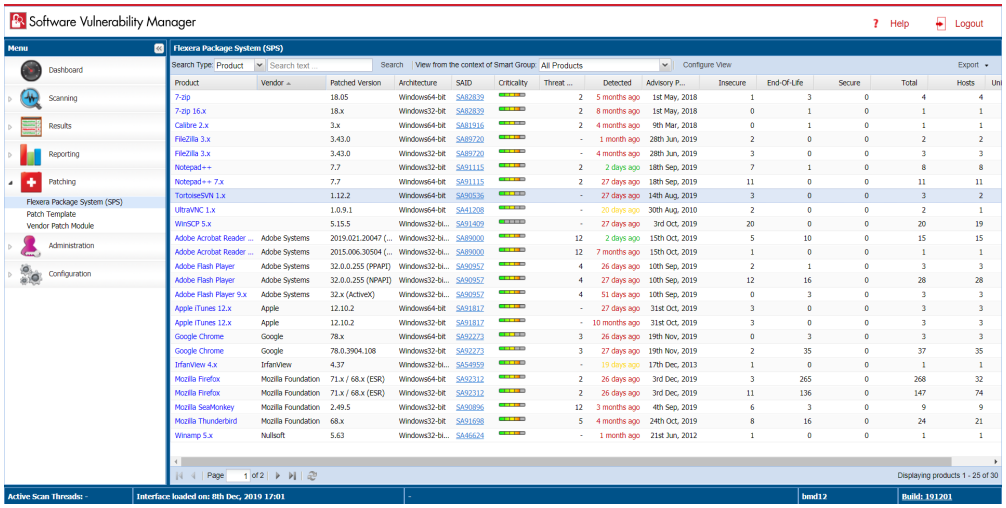


Extended Support in Non IE Browser

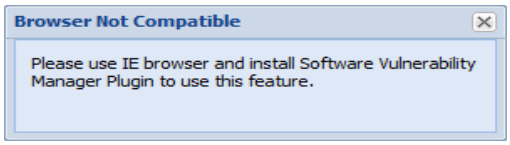
In Software Vulnerability Manager 2019, list of products available in **Flexera Package System (SPS)** and **Patch Template** can also be seen in non IE browsers.

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.*



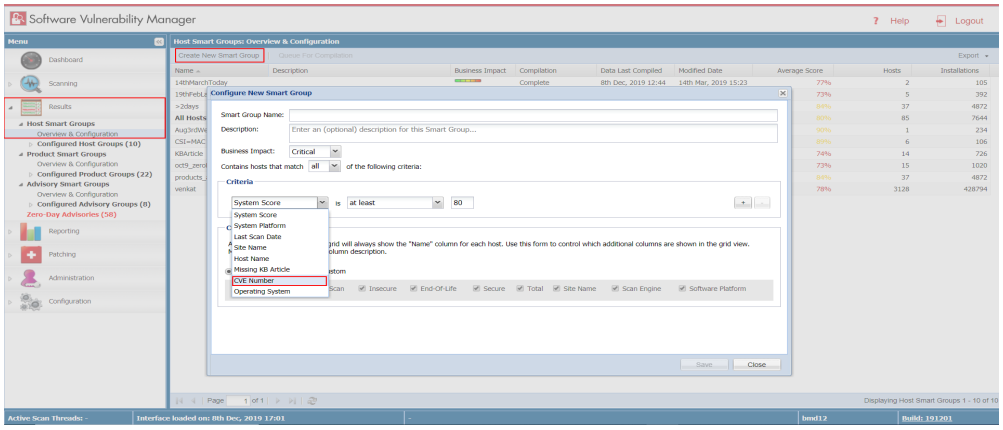
CVE Number as Criteria in Host Smart Groups

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:



Resolved Issues

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

Issue	Description
IOJ-1921584	SG Notification throws unexpected error if SG having special characters in its name is selected .
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 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:
  - New CRL distribution URLs:
    - http://*.amazontrust.com
    - http://s.ss2.us
  - If you require explicit URLs then allow below URLs:
    - http://crl.rootca1.amazontrust.com
    - http://crl.sca1b.amazontrust.com
    - http://crl.rootg2.amazontrust.com
    - http://s.ss2.us
  - Product URLs:
    - https://csi7.secunia.com
    - https://agent.csi7.secunia.com
    - https://dl.csi7.secunia.com
    - https://*.secunia.com
  - TimeStamp URL:
    - http://timestamp.digicert.com

Note • *We recommend whitelisting by domain name (timestamp.digicert.com), but if you are required to whitelist by IP, the IP address will be: 216.168.244.9.*

- 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.