Software Vulnerability Manager 2019 (Cloud Edition)
Release Notes

October 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:

- New Versioning Guidelines
- View Installations and Patch Information
- Vendor Patch Module - Configure View Enhanced
- Mac Agent Support

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).*

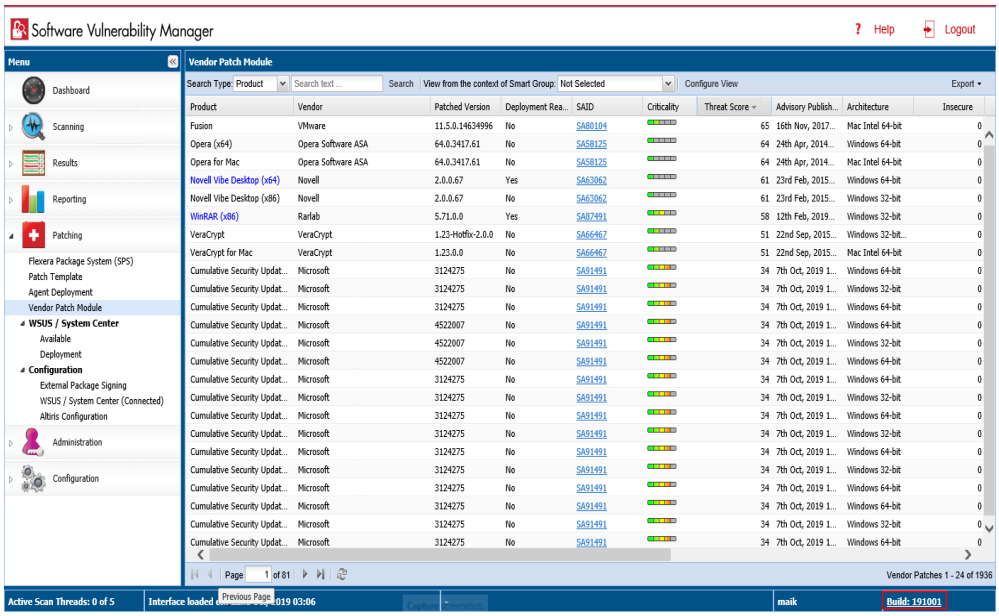
New Versioning Guidelines

Following the move to AWS infrastructure, customers can expect more frequent updates to Software Vulnerability Manager 2019 (Cloud Edition). With this in mind versioning guidelines have been changed to adopt the build number method.

The build number consist of 6 digits in the below format; for example, if the build number is **191001**:

- **19** - First two digit defines the year (2019)
- **10** - Second two digit defines the month (October)
- **01** - Last two digits is a counter of the number of releases done on that month (01 is the first, 02 is the second, etc.)

You can find the build number of your application in the right corner of the status bar as shown below.



View Installations and Patch Information

In Software Vulnerability Manager 2019, 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 in non IE browser (Chrome, Mozilla, etc.), Open **Patching > Vendor Patch Module**, you can see the list of products.

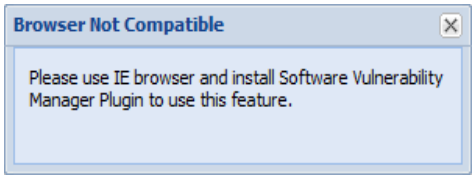
Right click a product, you can see the following options:

- 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.*

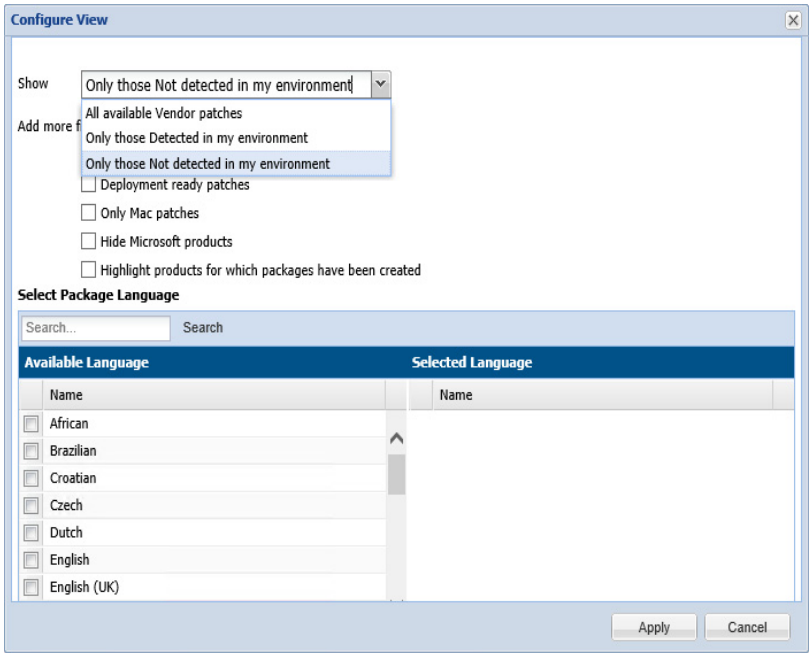


- *To learn more about the Vendor Patch Module, click here.*
- *To learn more about creating patches using the Vendor Patch Module, click here.*

Vendor Patch Module - Configure View Enhanced

In Software Vulnerability Manager 2019, 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



Mac Agent Support

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

Resolved Issues

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

Issue	Description
IOJ-2068477	RHEL 8 Agent Support
IOJ-1992395	Unexpected Error after editing the smart groups
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.

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
- First-Party cookie settings at least to Prompt (in Internet Explorer)
- Allow session cookies
- A PDF reader

Legal Information

Copyright Notice

Intellectual Property

Restricted Rights Legend