Software Vulnerability Manager 2019 (Cloud Edition)
Release Notes

November 2019

Introduction 1

New Features and Enhancements 1

Timestamping Services - DigiCert 2

Resolved Issues 2

Product Feedback 3

System Requirements 3

Legal Information 4

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 feature and enhancement:

- Timestamping Services - DigiCert

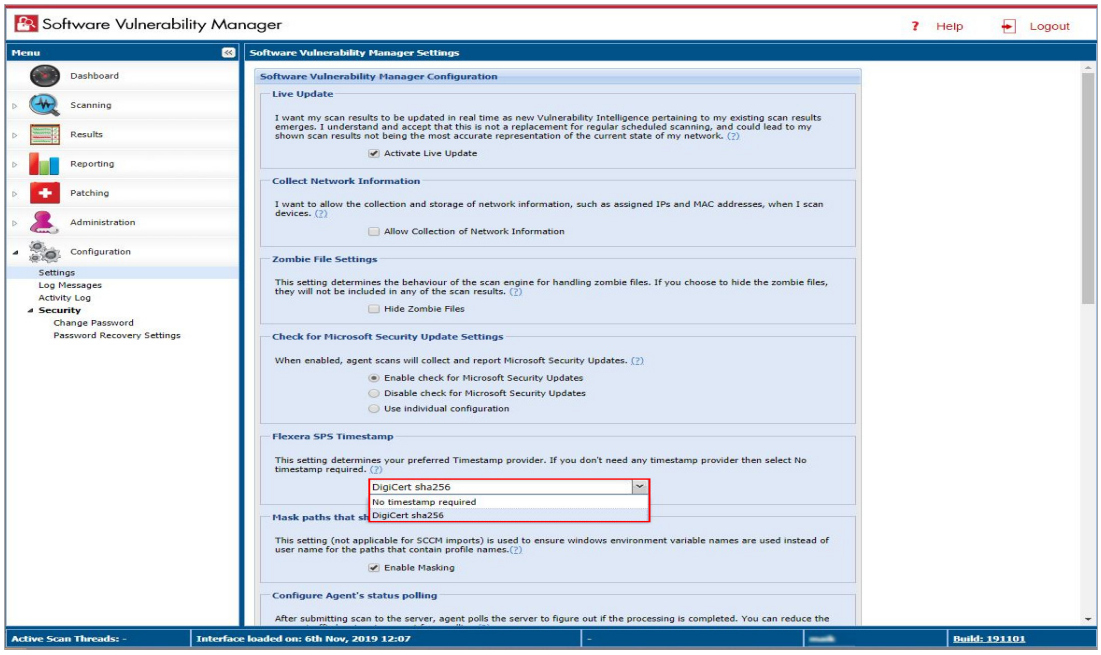
Note • *To see the following new feature and enhancement in your Software Vulnerability Manager 2019 interface, you must refresh your browser's cache (press Ctrl+F5).*

Timestamping Services - DigiCert

In Software Vulnerability Manager 2019, 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

There is no resolved issue in this release.

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.