

Software Vulnerability Manager 2019 R4 (Cloud Edition) Release Notes

August 2019

Introduction	1
New Features and Enhancements	2
Software Vulnerability Manager Data Center Move.....	2
CVE Search in Advisory Smart Groups.....	2
Resolved Issues.....	2
Product Feedback	3
System Requirements	3
Legal Information	3

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 R4 (Cloud Edition) includes the following new features and enhancements:

- Software Vulnerability Manager Data Center Move
- CVE Search in Advisory 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).

Software Vulnerability Manager Data Center Move

Software Vulnerability Manager infrastructure has moved from Copenhagen-based data center to Amazon Web Services (AWS) in Ireland for increased security, performance and stability.

For more information please visit Flexera community page at <https://community.flexera.com/t5/Software-Vulnerability/SVM-Data-Center-move/ba-p/105589>

CVE Search in Advisory Smart Groups

In Software Vulnerability Manager 2019 R4, you can now search for an advisory using CVE (CSIL- 8692).

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.

ADVIS	Advisory Description	Criticality	Threat Score	Zero-Day	Advisory Published	Vulnerabilities	Solution Status	CVSS Base Score	CVSS2 Base Score
SA41883	Microsoft Windows OLE Object Handl...	High	70	Yes	22nd Oct, 2014	2	Vendor Patched	9.8	10
SA47287	Microsoft Windows Server 2016 / Wind...	High	70	Yes	12th Mar, 2019	31	Vendor Patched	9.8	9
SA46671	Microsoft Windows Server 2012 / Wind...	High	57	Yes	11th Dec, 2018	10	Vendor Patched	9.8	0
SA46719	Microsoft Internet Explorer Memory Co...	High	52	Yes	20th Dec, 2018	1	Vendor Patched	9.8	0
SA49289	VLC Multiple Vulnerabilities	High	51	No	27th May, 2019	29	Vendor Patched	9.8	0
SA49324	Microsoft Windows Server 2016 / Wind...	High	44	Yes	9th Jul, 2019	39	Vendor Patched	9.8	0
SA49678	Microsoft Windows Server 2012 / Wind...	High	23	No	15th Aug, 2018	15	Vendor Patched	9.8	5
SA17125	Red Hat update for libxml2	High	12	No	24th Jun, 2016	18	Vendor Patched	9.8	10
SA49679	Mozilla Thunderbird Multiple Vulnerabi...	High	12	No	22nd May, 2019	15	Vendor Patched	9.8	0
SA49350	Apple Safari Multiple Vulnerabilities	High	12	No	14th May, 2019	21	Vendor Patched	9.8	0
SA46242	Microsoft Multiple Products Multiple Vul...	High	9	No	13th Nov, 2018	11	Vendor Patched	9.8	0
SA49497	Mozilla SeaMonkey Multiple Vulnerabilit...	High	7	No	27th Jul, 2018	11	Vendor Patched	9.8	0
SA17245	FileZilla Server OpenSSL Multiple Vulne...	High	7	No	28th Oct, 2016	7	Vendor Patched	7.8	7.8
SA47867	Microsoft Internet Explorer Multiple Vul...	High	7	No	12th Mar, 2019	22	Vendor Patched	9.8	9
SA48058	Apple iTunes Multiple Vulnerabilities	High	7	No	26th Mar, 2019	19	Vendor Patched	9.8	0
SA49526	Microsoft Edge Multiple Vulnerabilities	High	6	No	8th Jan, 2019	5	Vendor Patched	9.8	0
SA49529	Red Hat update for libssh2	High	5	No	2nd Jul, 2019	4	Vendor Patched	7.8	0
SA48499	Microsoft Multiple Products Multiple Vul...	High	5	No	9th Oct, 2018	5	Vendor Patched	9.8	0
SA49378	Microsoft Multiple Products Multiple Vul...	High	5	No	14th May, 2019	4	Vendor Patched	9.8	0
SA17561	Red Hat update for gnutils	High	5	No	21st Mar, 2017	4	Vendor Patched	7.8	7.8
SA49374	Red Hat update for kernel	High	5	No	18th Jun, 2018	4	Vendor Patched	7.8	9

Resolved Issues

There is no resolved issues 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://flexeracomunity.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:
 - 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

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.