Software Vulnerability Manager 2018 R2 (Cloud Edition)

(formerly Corporate Software Inspector)

Release Notes

May 2018

Introduction

Flexera’s Software Vulnerability Manager 2018 is a Vulnerability and Patch Management Software Solution that facilitates a customized Patch Management process. It combines Vulnerability 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 it enables proactive detection and remediation of vulnerabilities before they are actively exploited and your security compromised. With Software Vulnerability Manager 2018, 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 2018 integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager.

New Features and Enhancements

Software Vulnerability Manager 2018 R2 (Cloud Edition) includes the following new features and enhancements:

- Product Name Change - Software Vulnerability Manager 2018
- General Data Protection Regulation (GDPR) Compliance
- Support for CVSS version 3 score
- Storing of missing/installed KBs reported for each scan
- Reporting of domain site name for Mac OS X devices
- New view to support reporting of IP/MAC address

Note • *To see the following new features and enhancements in your Software Vulnerability Manager 2018 interface, you must refresh your browser's cache.*

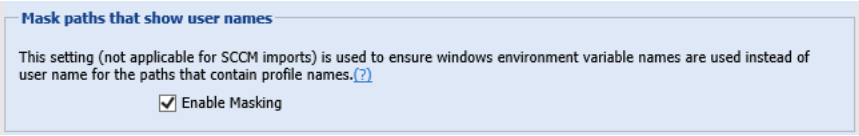
Product Name Change - Software Vulnerability Manager 2018

Over the years, we have had great feedback from our customers that they are interested in building repeatable processes for the management of software vulnerabilities. As the product has evolved, we have outgrown our original name of Corporate Software Inspector. As you know, this powerful solution goes far beyond software inspection. To better reflect its broader scope, **we are changing this solution's name from "Corporate Software Inspector" to "Software Vulnerability Manager"**. This change is a superficial one, but it helps better convey our solution as the complete vulnerability management solution that it represents. For more on where we started, are today and plan to go with Software Vulnerability Manager, read this short article on this change at our blog.

General Data Protection Regulation (GDPR) Compliance

To comply with the European Union's General Data Protection Regulation (GDPR), folder names that contain user names (Example: `C:\Documents and Settings\Username`) are now referenced using environment variables instead of hard-coded paths (Example: `%HOMEPATH%`).

In **Configuration > Settings > Mask paths that show user names**, users can select **Enable Masking** to turn on the GDPR functionality of masking user name information (CSIL-8552).



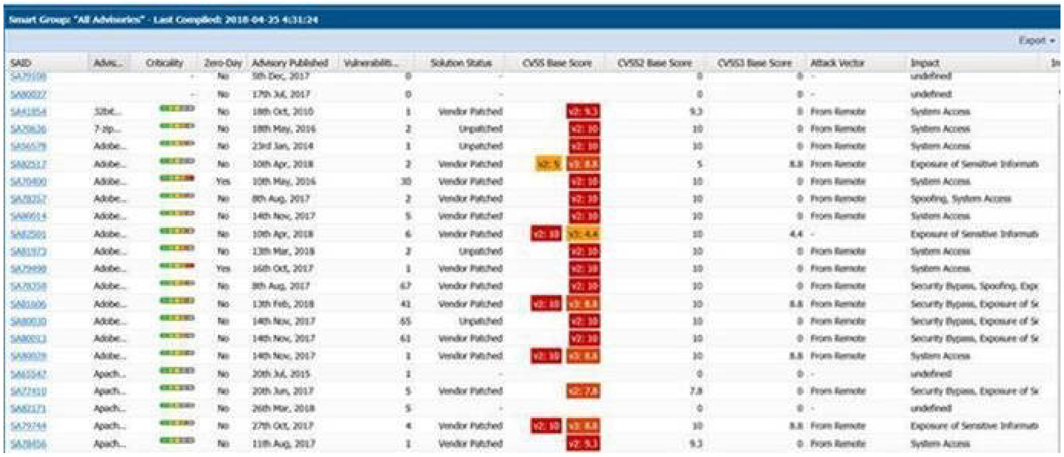
Mask paths that show user names

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

Support for CVSS version 3 score

Support has been added to display CVSS scores using the newer v3 standard. Starting on May 18th, Flexera's Secunia Research will begin entering all new CVSS scores using the v3 standard. Once we begin supplying CVSS v3 scores, you will be able to differentiate them from v2 score visually; values will be preceded by a "v2" or "v3" to indicate the scoring standard used to generate the value as indicated below (CSIL- 8589).



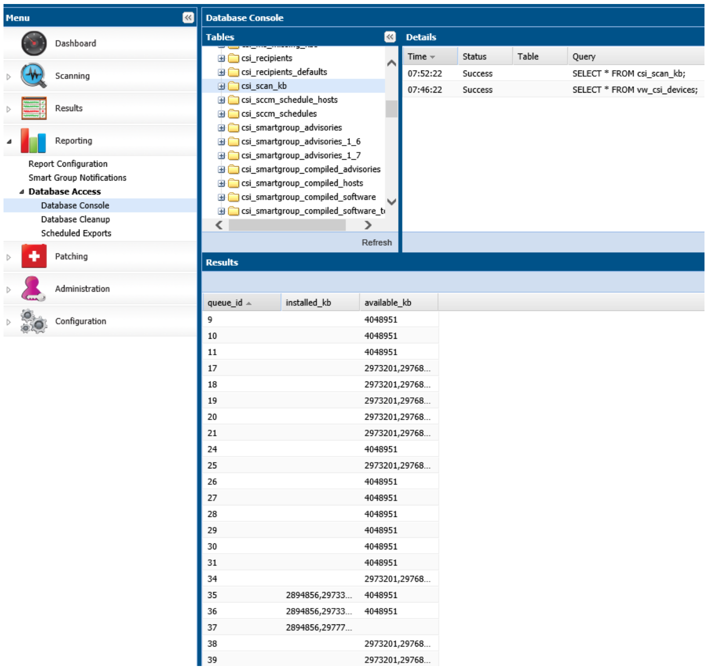
Smart Group: "All Advisories" - Last Compiled: 2018-04-25 4:31:24

SAID	Advis...	Criticality	Zero-Day	Advisory Published	Vulnerabili...	Solution Status	CVSS Base Score	CVSS2 Base Score	CVSS3 Base Score	Attack Vector	Impact	In
SA79108		-	No	5th Dec, 2017	0	-		0	0	-	undefined	
SA80027		-	No	17th Jul, 2017	0	-		0	0	-	undefined	
SA41854	32bit...		No	18th Oct, 2010	1	Vendor Patched	v2: 9.3	9.3	0	From Remote	System Access	
SA70626	7-zip...		No	18th May, 2016	2	Unpatched	v2: 10	10	0	From Remote	System Access	
SA56579	Adobe...		No	23rd Jan, 2014	1	Unpatched	v2: 10	10	0	From Remote	System Access	
SA82517	Adobe...		No	10th Apr, 2018	2	Vendor Patched	v2: 5 v3: 8.8	5	8.8	From Remote	Exposure of Sensitive Informati	
SA70400	Adobe...		Yes	10th May, 2016	30	Vendor Patched	v2: 10	10	0	From Remote	System Access	
SA78257	Adobe...		No	8th Aug, 2017	2	Vendor Patched	v2: 10	10	0	From Remote	Spoofing, System Access	
SA80614	Adobe...		No	14th Nov, 2017	5	Vendor Patched	v2: 10	10	0	From Remote	System Access	
SA82501	Adobe...		No	10th Apr, 2018	6	Vendor Patched	v2: 10 v3: 4.4	10	4.4	-	Exposure of Sensitive Informati	
SA81973	Adobe...		No	13th Mar, 2018	2	Unpatched	v2: 10	10	0	From Remote	System Access	
SA79998	Adobe...		Yes	16th Oct, 2017	1	Vendor Patched	v2: 10	10	0	From Remote	System Access	
SA78258	Adobe...		No	8th Aug, 2017	67	Vendor Patched	v2: 10	10	0	From Remote	Security Bypass, Spoofing, Expo	
SA81606	Adobe...		No	13th Feb, 2018	41	Vendor Patched	v2: 10 v3: 8.8	10	8.8	From Remote	Security Bypass, Exposure of Se	
SA80010	Adobe...		No	14th Nov, 2017	65	Unpatched	v2: 10	10	0	From Remote	Security Bypass, Exposure of Se	
SA80013	Adobe...		No	14th Nov, 2017	61	Vendor Patched	v2: 10	10	0	From Remote	Security Bypass, Exposure of Se	
SA80029	Adobe...		No	14th Nov, 2017	1	Vendor Patched	v2: 10 v3: 8.8	10	8.8	From Remote	System Access	
SA65547	Apach...		No	20th Jul, 2015	1	-		0	0	-	undefined	
SA77910	Apach...		No	20th Jun, 2017	5	Vendor Patched	v2: 7.8	7.8	0	From Remote	Security Bypass, Exposure of Se	
SA82171	Apach...		No	26th Mar, 2018	5	-		0	0	-	undefined	
SA79744	Apach...		No	27th Oct, 2017	4	Vendor Patched	v2: 10 v3: 8.8	10	8.8	From Remote	Exposure of Sensitive Informati	
SA78456	Apach...		No	11th Aug, 2017	1	Vendor Patched	v2: 9.3	9.3	0	From Remote	System Access	

For more on CVSS, see https://nvd.nist.gov/vuln-metrics/cvss

Storing of missing/installed KBs reported for each scan

Missing and installed KBs reported by scans will be stored in a new table "`csi_scan_kb`". This data will help debug vulnerabilities for Microsoft products. Users can export this data via the **Database Console** under **Reporting** (CSIL-8510).



Time ▾	Status	Table	Query
07:52:22	Success		SELECT * FROM csi_scan_kb;
07:46:22	Success		SELECT * FROM vw_csi_devices;

queue_id ▴	installed_kb	available_kb
9		4048951
10		4048951
11		4048951
17		2973201,29768...
18		2973201,29768...
19		2973201,29768...
20		2973201,29768...
21		2973201,29768...
24		4048951
25		2973201,29768...
26		4048951
27		4048951
28		4048951
29		4048951
30		4048951
31		4048951
34		2973201,29768...
35	2894856,29733...	4048951
36	2894856,29733...	4048951
37	2894856,29777...	
38		2973201,29768...
39		2973201,29768...

Reporting of domain site name for Mac OS X devices

If the Active Directory integration option has been enabled, then the Mac OS X Agent will report the actual domain name for the site name (CSIL-8446).

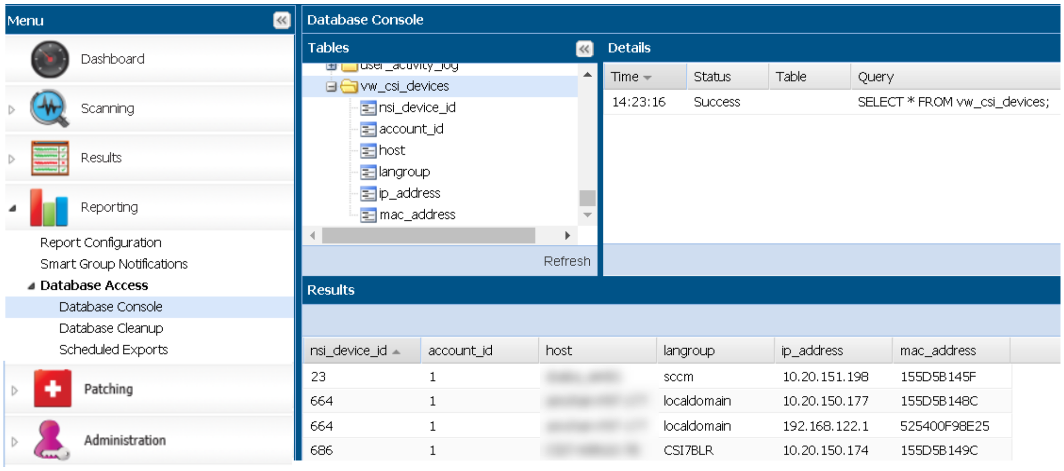
***Note** • The Mac OS X Agent has to be installed by the user who has access to read domain information.*

As of this release, Software Vulnerability Manager 2018 supports the following Mac OS X systems:

- 10.8 Mountain Lion
- 10.9 Mavericks
- 10.10 Yosemite
- 10.11 El Capitan
- 10.12 Sierra

New view to support reporting of IP/MAC address

Currently if users have selected to **Allow Collection of Network Information**, they can access the IP/MAC addresses reported in the latest assessment via the table “`vw_csi_devices`” (CSIL-8627).



Time	Status	Table	Query
14:23:16	Success		SELECT * FROM vw_csi_devices;

nsi_device_id	account_id	host	langroup	ip_address	mac_address
23	1	[redacted]	sccm	10.20.151.198	155D5B145F
664	1	[redacted]	localdomain	10.20.150.177	155D5B148C
664	1	[redacted]	localdomain	192.168.122.1	525400F98E25
686	1	[redacted]	CSI7BLR	10.20.150.174	155D5B149C

Resolved Issues

Software Vulnerability Manager 2018 R2 (Cloud Edition) has resolved the following issues:

- Mac OS X Agent fix for Google Drive
- Automatic logout after a password change

Mac OS X Agent fix for Google Drive

Certain Mac machines installed with MenuMeters, Google Drive, or Box failed to scan using the SVM2018 Mac OS X Agent. This issue has been resolved (CSIL-8387).

Automatic logout after a password change

When users change their password, they will automatically be logged out of Software Vulnerability Manager 2018. This security measure helps prevent an attacker from remaining logged in on a separate computer after discovering the user's initial username and password (CSIL-8598).

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 2018 console, your system should meet the following requirements:

- Minimum resolution: 1024x768
- 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://*.ws.symantec.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

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.

Disclaimer

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. The provision of such information does not represent any commitment on the part of Flexera. Flexera makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Flexera shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The software described in this document is furnished by Flexera under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software, except as specifically allowed in the license agreement. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to: photocopying, recording, or information recording and retrieval systems, for any purpose other than the purchaser’s personal use, without the express, prior, written permission of Flexera.