Flexera

Software Vulnerability Manager 2019

API User Guide

Legal Information

Book Name: Software Vulnerability Manager API Guide

Part Number: SVM-2019-API01

Product Release Date: July 2019

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.

Contents

1

Software Vulnerability Manager 2019 API Help Library

This API User Guide provides the API information for Flexera's Software Vulnerability Manager

Table 1-1 • Software Vulnerability Manager API Help Library

Topic	Content
API Introduction	This section describes how to access the API information.
Login API	This section provides the Software Vulnerability Manager API information for server login.
Completed Scan API Information	This section provides the Software Vulnerability Manager API information for Completed Scan API.
Host Smart Group API Information	This section provides the Software Vulnerability Manager API information for Host Smart Groups module.
Product Smart Group API Information	This section provides the Software Vulnerability Manager API information for Product Smart Groups module.
Advisory Smart Group API Information	This section provides the Software Vulnerability Manager API information for Advisory Smart Groups module.
Appendix A - Sample API Code	This section provides the sample powershell code to get Host details

Using Help

Help is available from the Software Vulnerability Manager interface help icon located at the top right of the screen.

Online Help

For online help, see https://helpnet.flexerasoftware.com/svm/Default.htm

Release Notes

For the latest release notes, see https://helpnet.flexerasoftware.com/?product=Software%20Vulnerability%20Manager&version=Current

For earlier release notes, see https://helpnet.flexerasoftware.com/?product=Software%20Vulnerability%20Manager&version=Previous

Contact Us

Flexera is headquartered in Itasca, Illinois, and has offices worldwide. To contact us or to learn more about our products, visit our website at:

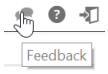
https://www.flexera.com/

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 Customer Community feedback page for Software Vulnerability Manager.

Note • *You will need your Flexera Customer Community credentials to enter feedback.*

You can also submit feedback through the Software Vulnerability Manager user interface by clicking the feedback icon in the upper-right-hand corner of each module.



2

API Introduction

The purpose of this document is to help customers leverage internal APIs used by Software Vulnerability Manager website to pull data via custom code. This document assumes the reader has some programming experience. A sample of code has been provided as an Appendix. These APIs provides a simple way to automate the data collection from Software Vulnerability Manager. Customers can choose to extend their custom code to access data across multiple login and across multiple partitions to create integrated reports. Customers could also choose to engage Flexera services to create maintainable custom reports.

API used in Software Vulnerability Manager are currently not restful. This means you have to provide login credentials for an account and derive a token that identifies the account.

This section provides an overview of the following API topics:

- How to get the Token
- How to use the API

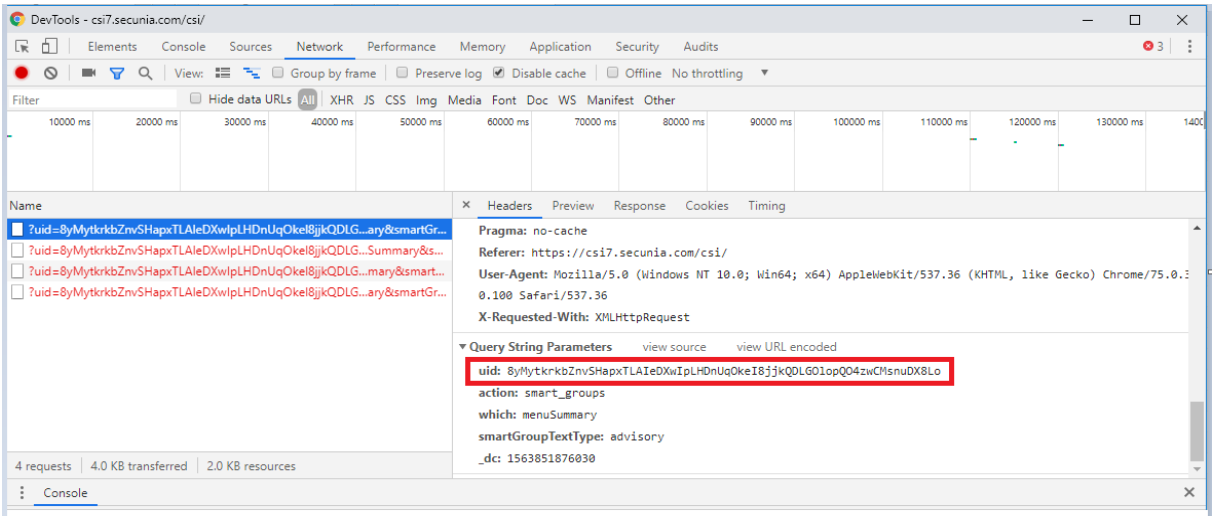
How to get the Token

You need to Login using the Software Vulnerability Manager credentials to get the Token.

To know more about the Login API information see Login API Information

Task ***To Receive the Token Using Browser***

1. You can use your browser to inspect the transactions happening between the browser and the web server.
2. Enter the link https://csi7.secunia.com/csi/# in your web browser and press F12. The below screen appears.



3. Enter your credentials and click Login.
4. After successful login, you can find the Token in the **Query String Parameter** in **uid:**
5. Enter the **Token** as `uid=<Enter Token>` in the API URL in your subsequent transactions.

How to use the API

Software Vulnerability Manager APIs are divided into below sections:

- Server url
- uid
- action
- which
- smartGroupTextType

Sample API URL for **Product Smart Groups >> Overview & Configuration** is shown below:

https://csi7.secunia.com/csi/api/

?uid=zIw6KAA70AGELYjDJmjI2gjEt9WbKoPSRKhpLy9NRVdWzumsuXMNa0eEarcXa0To

&action=smart_groups

&which=menuSummary

&smartGroupTextType=product

Note • *Note the following:*

- *API may or may not have all the sections however few parameters like smartGroupId, productID from the JSON response from the parent API.*
- *Enter the token in the uid section*

3

Login API

This API helps you to login to the Software Vulnerability Manager server and generate token that can be used for subsequent transactions.

This section includes the following:

- Login API Information

Login API Information

The first step is to login to the Software Vulnerability Manager. UID value received from the successful login must be used in the subsequent transactions

Informations required to Login is organized into the following tabs:

Table 3-1 • Login API Information

Requirement Type	Details
API	*https://csi7.secunia.com/csi/api/?*uid=&action=manuallogin
Method	POST
Parameters	• username • password ***Note*** • *Enter the SVM cloud login credentials*

Table 3-1 • Login API Information

Requirement Type	Details

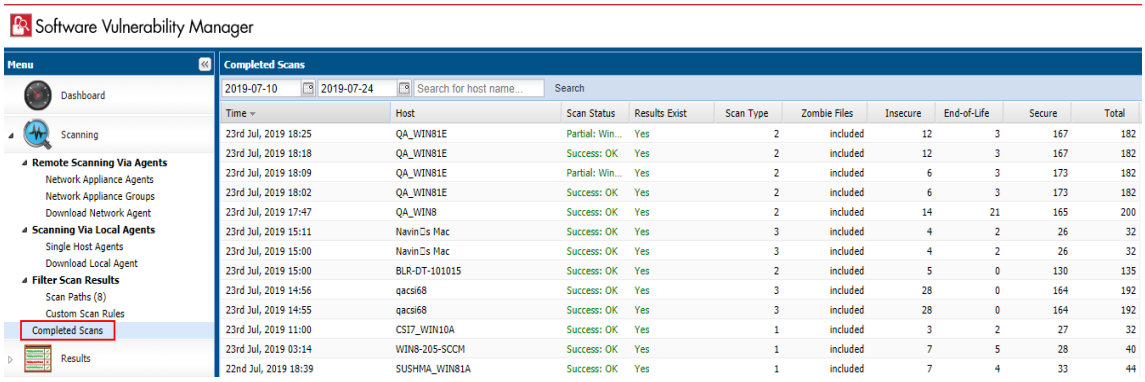
Response	**Valid Credential**
	`{"success":true,"response":1,"reason":"Login successful",`
	`"uid":"eNC4bgWbaumKxF0iqyRDcAsVOQ0NBpa5KxCynq5p3lzIzsrF8TKiYijIHxRfS4Bj"}`
	
	Invalid Credential
	`{"success":true,"response":2,"reason":"Invalid Credentials."`

Received Information	UID value ***Note*** • *UID value of successful response can be used in the API uid section for the subsequent transactions as shown below* *https://csi7.secunia.com/csi/api/?uid=<UID of successful login reponse>*

4

Completed Scan API Information

This API helps to capture the data from Completed Scans page in Software Vulnerability Manager.



This section includes the following:

- List All the Host and Scan Status
- List Scan Result for Each Host

List All the Host and Scan Status

This section describes the API information to view the following details from Completed Scan page:

- Host details
- Scan Status
- Results Exist
- Scan Type
- Zombie Files
- Insecure

- End-of-Life
- Secure

The information required to view the **Completed Scans** is organized into the following tabs:

Table 4-1 • List of Host and Scan Status API Information

Requirement Types	Details
API URL	https://csi7.secunia.com/csi/api/?uid=**<xyz>**&action=**<xyz>**&which=**<xyz>**  ***Note*** • *The value for* **<XYZ>** *in the above API is defined in the Parameters section*
Parameters	uid = UID Value taken from successful login see How to get the Token action = csi_completed_scans which = overview  ***Note*** • *These parameters have to be entered in the* **<XYZ>** *of above API respectively*
Sample Sort	&sort=status_date&dir=DESC&sorters=%5B%7B%22field%22%3A%22status_date%22%2C%22direction%22%3A%22DESC%22%7D%5D&from=2019-07-09%2018%3A30%3A00&to=2019-07-24%2018%3A30%3A00&host=&start=0&limit=21
Methods	GET
Sample JSON Response	{"success":true,"error_code":0,"data":{"rows":[{"nsi_device_id":"736","status_date":"2019-07-23 12:55:41","host":"QA_WIN81E","langroup":"SCCM","scan_type":"2","short_msg":"Partial: Windows Update failed","long_msg":"The scan was partially successful. An error occurred during the Windows Update check.\\n\\nIt appears that the RPC service is not running or that the Host is firewalled to disallow access to the RPC service.\\n\\nNOTE: This means that certain Microsoft products for this Host, are listed with a potential incorrect security state.","no_insecure":"12","no_eol":"3","no_patched":"167","no_total":"182","no_zombie":"included","id":"18577","software_inspector_id":"21","results_exist":"1"},{"nsi_device_id":"736","status_date":"2019-07-23 12:48:14","host":"QA_WIN81E","langroup":"SCCM","scan_type":"2","short_msg":"Success: OK","long_msg":"Scan executed successfully","no_insecure":"12","no_eol":"3","no_patched":"167","no_total":"182","no_zombie":"included","id":"18576","software_inspector_id":"21","results_exist":"1"},...
Received Information	Time, Host Name, Scan Status, Results Exist, Device ID, etc.

List Scan Result for Each Host

This section describes the API information to view the **List Scan result for Each Host**

The information required to view the **Scan result** for each Host is organized into the following tabs:

Table 4-2 • Scan Result of each Host API Information

Requirement Types	Details
API URL	https://csi7.secunia.com/csi/api/?uid=**<xyz>**&action=**<xyz>**&which=**<xyz>**  ***Note*** *• The value for* **<XYZ>** *in the above API is defined in the Parameters section*
Parameters	uid = UID Value taken from successful login see How to get the Token action = hosts which = get_host_scan_results  ***Note*** *• These parameters have to be entered in the* **<XYZ>** *of above API respectively*
Methods	POST
Sample JSON Response	`"success":true,"error_code":0,"data":[{"product_id":"62259","product_name":"7-zip 19.x","version":"19.0.0.0","state":"Secure","vuln_id":"-","vuln_title":"-","vuln_criticality":"-","vuln_threat_score":"","vuln_create_date":"-","vuln_count":"-","vuln_cvss_score":"","vuln_cvss3_score":"","vuln_cvss_score_all":"","path":"C:\\Program Files (x86)\\7-Zip\\7z.exe","vendor_name":"","direct_download":"","secure_version":"","missing_ms_kb":"","soft_type":"2","vpm_id":""},{"product_id":"62259","product_name":"7-zip 19.x","version":"19.0.0.0","state":"Secure","vuln_id":"-","vuln_title":"-","vuln_criticality":"-","vuln_threat_score":"","vuln_create_date":"-","vuln_count":"-","vuln_cvss_score":"","vuln_cvss3_score":"","vuln_cvss_score_all":"","path":"C:\\Program Files\\7-Zip\\7z.exe","vendor_name":"","direct_download":"","secure_version":"","missing_ms_kb":"","soft_type":"2","vpm_id":"8"},{"product_id":"56678","product_name":"Adobe Brackets 1.x","version":"1.14.0.0","state":"Secure","vuln_id":"-","vuln_title":"-","vuln_criticality":"-","vuln_threat_score":"","vuln_create_date":"-","vuln_count":"-","vuln_cvss_score":"","vuln_cvss3_score":"","vuln_cvss_score_all":"","path":"C:\\Program Files (x86)\\Brackets\\Brackets.exe",...`
Received Information	Application Name, Version, State, SAID, Criticality, CVSS Base Score, Threat Score, etc.

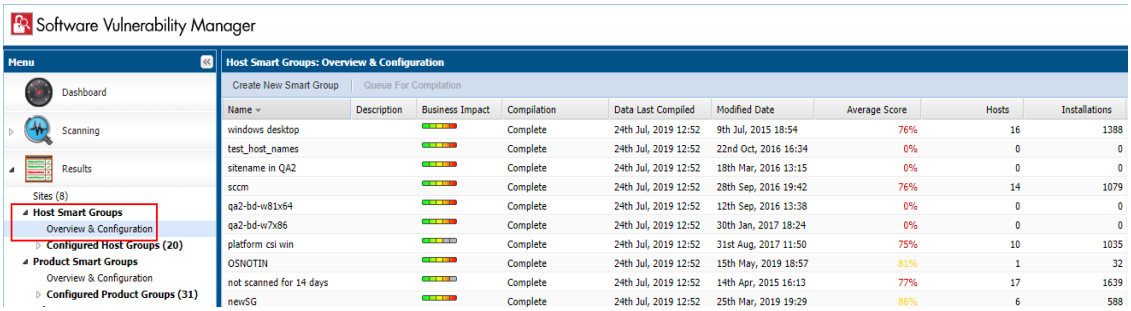
Table 4-2 • (cont.)Scan Result of each Host API Information

Requirement Types	Details
Sample Form Data	• start: 0 • limit: 27 • sort: product_name • dir: ASC • eol: true • patched: true • insecure: true • device_id: 1287 • sorters: product_name=ASC

5

Host Smart Group API Information

This API helps to capture the data from the Host Smart Groups page in Software Vulnerability Manager.



This section describes the API information for the following:

- Host Smart Groups API
- Configured Host Groups API

Host Smart Groups API

The information required to view the **Host Smart Groups** is organized into the following tabs:

Table 5-1 • Host Smart Group API Information

Requirement Types	Details
API	***https://csi7.secunia.com/csi/api/ ?uid=<xyz>&action=<xyz>&which=<xyz>smartGroupTextType=<xyz>&_dc=1 563347478676*** ***Note*** • *The value for* **<XYZ>** *in the above API is defined in the Parameters section*

Table 5-1 • Host Smart Group API Information

Requirement Types	Details
Methods	GET
Parameters	uid = UID Value taken from successful login see How to get the Token action = **smart_groups** which = **menuSummary** smartGroupTextType = **host**  ***Note*** • *These parameters have to be entered in the* **<XYZ>** *of above API respectively*
Response	{"success":true,"error_code":0, "data": {"rows":[{"id":"1","name":"All Hosts","editable":"0","description":"Smart Group containing all Hosts (default Flexera Smart Group). Note: Smart Group is NOT editable.","logic_type":"all","business_impact":"2","custom_columns":"","all_custom_columns":"1","date_modified":"2019-06-03 10:16:18","in_progress":"0","generate_asap":"0","compiled_time":"2019-07-16 10:31:35","hosts":"1","average_score":"88","num_installations":"219"} , {"id":"11","name":"Test1","editable":"1","description":"Test1","logic_type":"all","business_impact":"1","custom_columns":"","all_custom_columns":"1","date_modified":"2019-07-16 09:52:50","in_progress":"0","generate_asap":"0","compiled_time":"2019-07-16 10:31:35","hosts":"1","average_score":"88","num_installations":"219"}] ,"total":2}}  ***Note*** • *The numerical value received as* ***"id":"n"*** *from the JSON response is the* ***smartGroupId*** *parameter for Configured Host Groups API, where "n" is the numerical number*
Received Information	Name, Description, Business Impact, Compilation, Data Last Compiled, Average Score, Hosts, Installations, Host ID, Total number etc.

Configured Host Groups API

The information required to read the each **Host Smart Group** is organized into the following tabs:

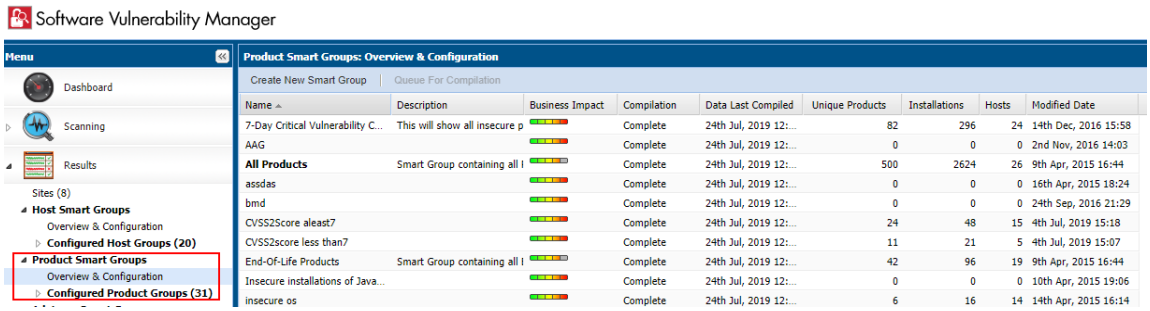
Table 5-2 • Configured Host Groups API Information

Requirement Types	Details
API	***https://csi7.secunia.com/csi/api/ ?uid=<xyz>&action=<xyz>&which=<xyz>smartGroupTextType=<xyz>&smartGroupId=<xyz>&_dc=1563355275960&sort=host_name&dir=ASC&sorters=%5B%7B%22field%22%3A%22host_name%22%2C%22direction%22%3A%22ASC%22%7D%5D&host_name=&start=0&limit=21***  ***Note*** • *The value for* **<XYZ>** *in the above API is defined in the Parameters section*
Methods	GET
Parameters	uid = UID Value taken from successful login see How to get the Token action = **smart_groups** which = **getSmartGroupContents** smartGroupTextType = **host** smartGroupId = ***"id":"n"*** value from the JSON response of Host Smart Groups API  ***Note*** • *The above parameters have to be entered in the* **<XYZ>** *of above API respectively*
Response	`{"success":true,"error_code":0,"data":{"rows":[{"nsi_device_id":"1","host_name":"BLR-LT-101247","score":"88","num_insecure":"22","num_eol":"4","num_patched":"193","num_installations":"219","group_name":"FLEXERA","software_inspector_id":"21","updated":"2019-07-12 07:07:26","software_inspector_version":"7.6.1.2"}],"total":"1"},"compiledTime":"2019-07-17 00:28:04"}`
Received Information	Host Name, System Score, Last Scan, Insecure, End-of-Life, Secure, Total, Site Name, Scan Engine, Software Platform etc.

6

Product Smart Group API Information

This API helps to capture the data from the Product Smart Groups page in Software Vulnerability Manager.



This section describes the API information for the following:

- Product Smart Group API
- Configured Product Groups API
- View Installations API - Products

Product Smart Group API

This information required to read the **Product Smart Group** scan results is organized into the following tabs:

Table 6-1 • Product Smart Group API Information

Required Types	Details
API	***https://csi7.secunia.com/csi/api/ ?uid=<xyz>&action=<xyz>&which=<xyz>smartGroupTextType=<xyz>&smartGroupId=<xyz>&_dc=1563357098636&sort=name&dir=ASC&sorters=%5B%7B%22field%22%3A%22name%22%2C%22direction%22%3A%22ASC%22%7D%5D&start=0&limit=21***  ***Note*** • *The value for* **<XYZ>** *in the above API is defined in the Parameters section*
Methods	GET
Parameters	uid = UID Value taken from successful login see How to get the Token action = **smart_groups** which = **overview** smartGroupTextType = **product**  ***Note*** • *The above parameters have to be entered in the* **<XYZ>** *of the above API respectively*

Table 6-1 • Product Smart Group API Information

Required Types	Details
Response	{"success":true,"error_code":0,"data":{"rows":[{"id":"2","name":"All Products","editable":"0","description":"Smart Group containing all Products (default Flexera Smart Group). Note: Smart Group is NOT editable.","logic_type":"all","business_impact":"2","custom_columns":"","all_custom_columns":"1","num_products":"75","num_installations":"219","num_hosts":"1","date_modified":"2019-06-03 10:16:18","compiled_time":"2019-07-17 00:28:05","in_progress":"0","generate_asap":"0"},{"id":"10","name":"CVSS2 less 3","editable":"1","description":"","logic_type":"all","business_impact":"1","custom_columns":"","all_custom_columns":"1","num_products":"2","num_installations":"4","num_hosts":"1","date_modified":"2019-06-03 11:21:23","compiled_time":"2019-07-17 00:28:07","in_progress":"0","generate_asap":"0"},{"id":"8","name":"CVSS3 Less than4","editable":"1","description":"CVSS3 Less than4","logic_type":"all","business_impact":"1","custom_columns":"","all_custom_columns":"1","num_products":"1","num_installations":"2","num_hosts":"1","date_modified":"2019-06-03 10:33:49","compiled_time":"2019-07-17 00:28:08","in_progress":"0","generate_asap":"0"} ***Note*** *• The numerical value received as* ***"id":"n"*** *from the JSON response is the* ***smartGroupId*** *parameter for Configured Product Groups API, where "n" is the numerical number*
Received Information	Name, Description, Business Impact, Compilation, Data Last Compiled, Unique Products, Installations, Hosts, Modified Date, etc.

Configured Product Groups API

The information required to read the each **Product Smart Group** results is organized into the following tabs:

Table 6-2 • Configured Product Groups API Information

Requirement Types	Details
API	***https://csi7.secunia.com/csi/api/ ?uid=<xyz>&action=<xyz>&which=<xyz>smartGroupTextType=<xyz>&smartGroupId=<xyz>&_dc=1563425993660&start=0&limit=20&sort=product_name&dir=ASC&sorters=%5B%7B%22field%22%3A%22product_name%22%2C%22direction%22%3A%22ASC%22%7D%5D&product_name=*** ***Note*** *• The value for* ***<XYZ>*** *in the above API is defined in the Parameters section*
Methods	GET

Table 6-2 • Configured Product Groups API Information

Requirement Types	Details
Parameters	uid = UID Value taken from successful login see How to get the Token action = **smart_groups** which = **getSmartGroupContents** smartGroupTextType = **product** smartGroupId = ***"id":"n"*** value from the JSON response of Product Smart Group API  ***Note*** • *These parameters have to be entered in the* **<XYZ>** *of the above API respectively*
Response	{"success":true,"error_code":0,"data":{"rows":[{"product_id":"60103","product_name":"7-zip 18.x","vendor_name":"","vuln_criticality":"-","vuln_id":"-","vuln_title":"-","vuln_cvss_score_all":"","vuln_cvss_score":"0","vuln_cvss3_score":"0","num_insecure":"0","num_eol":"0","num_patched":"2","num_installations":"2","num_hosts":"1","direct_download":"http:\/\/dl.secunia.com\/SPS\/7-Zip_18.05_32-bit_SPS.exe","secure_version":"18.05","soft_type":"2","vuln_threat_score":"","vpm_id":"9"},{"product_id":"16455","product_name":"ActiveTcl 8.x","vendor_name":"ActiveState","vuln_criticality":"-","vuln_id":"-","vuln_title":"-","vuln_cvss_score_all":"","vuln_cvss_score":"0","vuln_cvss3_score":"0","num_insecure":"0","num_eol":"0","num_patched":"1","num_installations":"1","num_hosts":"1","direct_download":"","secure_version":"","soft_type":"2","vuln_threat_score":"","vpm_id":""},{"product_id":"59498","product_name":"Adobe Acrobat Reader 2017 17.x","vendor_name":"Adobe Systems","vuln_criticality":"-","vuln_id":"-","vuln_title":"-","vuln_cvss_score_all":"","vuln_cvss_score":"0","vuln_cvss3_score":"0","num_insecure":"0","num_eol":"0","num_patched":"1","num_installations":"1","num_hosts":"1","direct_download":"http:\/\/dl.secunia.com\/SPS\/AdobeReader2017_2017.011.30142_MUI_SPS.exe","secure_version":"2017.011.30142","soft_type":"2","vuln_threat_score":"","vpm_id":"163"},  ***Note*** • *The numerical value received as* ***"product_id":"60068"*** *from the JSON response is the* ***productId*** *parameter for View Installations API - Products, where "n" is the numerical number*
Received Information	Product Name, Patch Version, SAID, Advisory Description, Criticality, Threat Score, CVSS Base Score, CVSS2 Base Score, CVSS3 Base Score, Vendor, Insecure, End-Of-Life, Secure, Total, Affected Hosts, Download Link, Product Type etc.

View Installations API - Products

This section explains API information to view the below details of any product:

- API to View the product **Overview Scan** see Product Overview Scan Info API
- API to view the product **Installations Scan** see Product Installations Scan Info API

Product Overview Scan Info API

The information required to view each **Product Overview Scan** results is organized into the following tabs:

Table 6-3 • Product Overview API Information

Requirement Types	Details
API	***https://csi7.secunia.com/csi/api/ ?uid=<xyz>&action=<xyz>&which=<xyz>&_dc=1563807741382&productId="n"&smartGroupId="n"***  ***Note*** • *The value for* **<XYZ>** *&* **"n"** *in the above API is defined in the Parameters section*
Methods	GET
Parameters	uid = UID Value taken from successful login see How to get the Token action = **results** which = **installationOverview** productID = **"product_id":"n"** value from the JSON response of Configured Product Groups API smartGroupId = **"id":"n"** value from the JSON response of Product Smart Group API  ***Note*** • *The above parameters have to be entered in the* **<XYZ>** *of above API respectively*
Response	`{"success":true,"error_code":0,"data":{"countEndOfLife":"0","countInsecure":"0","countPatched":"1","productName":"Adobe AIR 27.x","createdAt":"2017-09-20 23:48:59","versionsFound":true,"missingKBsFound":false,"uniq_totalcount_mskbs":[],"uniq_totalcount_versions":[]}}`
Received Information	State of Detected Installations

Product Installations Scan Info API

The information required to view each **Product Installations Scan** results is organized into the following tabs:

Table 6-4 • Product Installation Scan Info API Information

Requirement Types	Details
API	***https://csi7.secunia.com/csi/api/ ?uid=<xyz>&action=<xyz>&which=<xyz>&_dc=1563809090855&start=0&limit=14&sort=host&dir=ASC&product_id="n"&smartGroupId="n"&patched=true&end_of_life=true&insecure=true&sorters=%5B%7B%22field%22%3A%22host%22%2C%22direction%22%3A%22ASC%22%7D%5D*** ***Note*** • *The value for* **<XYZ>** *&* **"n"** *in the above API is defined in the Parameters section*
Methods	GET
Parameters	uid = UID Value taken from successful login see How to get the Token action = **results** which = **get_Installations** productID = **"product_id":"n"** value from the JSON response of Configured Product Groups API smartGroupId = **"id":"n"** value from the JSON response of Product Smart Group API ***Note*** • *The above parameters have to be entered in the* **<XYZ>** *of above API respectively*
Response	{"success":true,"error_code":0,"data":{"rows":[{"state":"1","nsi_device_id":"737","host":"BANGHV_QA_WIN8A","langroup":"SCCM","updated":"2019-07-04 08:39:58","version":"16.0.10730.20344","missing_ms_kb":"","path":"c:\\program files (x86)\\microsoft office\\root\\office16\\excel.exe","secure_status":"0","vuln_id":"86947","vuln_title":"Microsoft Multiple Products Multiple Vulnerabilities","vuln_criticality":"2","vuln_threat_score":"6"},{"state":"0","nsi_device_id":"732","host":"CSI7-WIN10-59","langroup":"SCCM","updated":"2019-07-04 08:39:14","version":"16.0.11727.20230","missing_ms_kb":"","path":"c:\\program files (x86)\\microsoft office\\root\\office16\\excel.exe","secure_status":"1","vuln_id":"-","vuln_title":"-","vuln_criticality":"-","vuln_threat_score":""},..

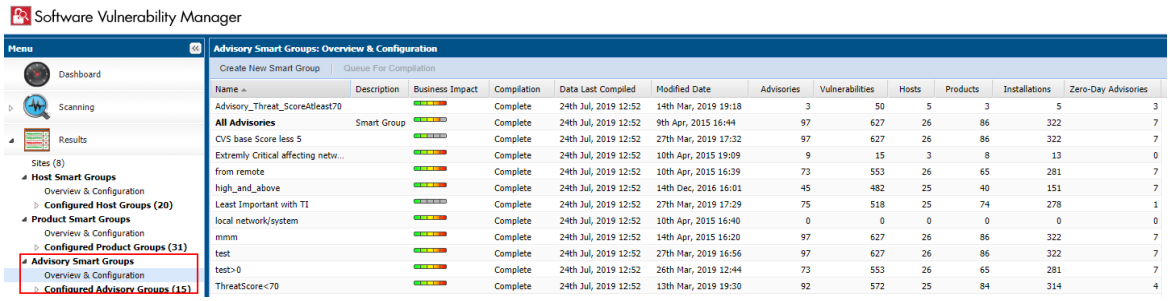
Table 6-4 • Product Installation Scan Info API Information

Requirement Types	Details
Received Information	Host details, SAID, Criticality, Threat Score, State, Version, Last Scan, Path, etc.  ***Note*** *• Threat Score is available only for users with Threat Intelligence module*

7

Advisory Smart Group API Information

This API helps to capture the data from the Product Smart Groups page in Software Vulnerability Manager.



This section describes the API information for the following:

- Advisory Smart Group API
- Configured Advisory Groups API

Advisory Smart Group API

The information required to read the **Advisory Smart Group** results is organized into the following tabs:

Table 7-1 • Advisory Smart Group API Information

Requirement Types	Details
API	**https://csi7.secunia.com/csi/api/ ?uid=<xyz>&action=<xyz>&which=<xyz>smartGroupTextType=<xyz>&_dc=1563433180691&sort=name&dir=ASC&sorters=%5B%7B%22field%22%3A%22name%22%2C%22direction%22%3A%22ASC%22%7D%5D&start=0&limit=20** ***Note*** *• The value for* **<XYZ>** *in the above API is defined in the Parameters section*
Methods	GET
Parameters	uid = UID Value taken from successful login see How to get the Token action = **smart_groups** which = **overview** smartGroupTextType = **advisory** sort = ***Note*** *• The above parameters have to be entered in the* **<XYZ>** *of the above API respectively*

Table 7-1 • (cont.)Advisory Smart Group API Information

Requirement Types	Details
Response	{"success":true,"error_code":0,"data":{"rows":[{"id":"6","name":"All Advisories","editable":"0","description":"Smart Group containing all Advisories (default Flexera Smart Group). Note: Smart Group is NOT editable.","logic_type":"all","business_impact":"2","custom_columns":"","all_custom_columns":"1","advisories":"17","vulnerabilities":"109","hosts":"1","products":"18","installations":"22","zero_day":"1","date_modified":"2019-06-03 10:16:18","in_progress":"0","generate_asap":"0","compiled_time":"2019-07-18 06:59:06"},{"id":"9","name":"CVSS3 Less than7","editable":"1","description":"CVSS3 Less than7","logic_type":"all","business_impact":"1","custom_columns":"","all_custom_columns":"1","advisories":"4","vulnerabilities":"7","hosts":"1","products":"4","installations":"5","zero_day":"0","date_modified":"2019-06-03 11:17:02","in_progress":"0","generate_asap":"0","compiled_time":"2019-07-18 06:59:06"},{"id":"7","name":"Zero-Day Advisories","editable":"0","description":"Smart Group containing all Zero-Day Advisories (default Flexera Smart Group). Note: Smart Group is NOT editable.","logic_type":"all","business_impact":"1","custom_columns":"","all_custom_columns":"1","advisories":"1","vulnerabilities":"39","hosts":"1","products":"1","installations":"1","zero_day":"1","date_modified":"2019-06-03 10:16:18","in_progress":"0","generate_asap":"0","compiled_time":"2019-07-18 06:59:06"}],"total":3}} ***Note*** *• The numerical value received as* ***"id":"n"*** *from the JSON response is the* ***smartGroupId*** *parameter for Configured Advisory Groups API, where "n" is the numerical number*
Received Information	Name, Description, Business Impact, Compilation, Data Last Compiled, Advisories, Vulnerabilities, Products, Installations, Hosts, Zero-Day Advisories etc.

Configured Advisory Groups API

The information required to view the each **Advisory Smart Group** results is organized into the following tabs:

Table 7-2 • Configured Advisory Groups API Information

Requirement Types	Details
API	***https://csi7.secunia.com/csi/api/ ?uid=<xyz>&action=<xyz>&which=<xyz>smartGroupTextType=<xyz>&smartGroupId=<xyz>&_dc=1563434762909&sort=vuln_title&dir=ASC&sorters=%5B%7B%22field%22%3A%22vuln_title%22%2C%22direction%22%3A%22ASC%22%7D%5D&start=0&limit=20***  ***Note*** *• The value for* **<XYZ>** *in the above API is defined in the Parameters section*
Methods	GET
Parameters	uid = UID Value taken from successful login see How to get the Token action = **smart_groups** which = **getSmartGroupContents** smartGroupTextType = **product** smartGroupId = ***"id":"n"*** value from the JSON response of Advisory Smart Group API sort =  ***Note*** *• These parameters have to be entered in the* **<XYZ>** *of the above API respectively*
Response	{"success":true,"error_code":0,"data":{"rows":[{"vuln_id":"87695","vuln_title":"Cisco Multiple Products Update Service Privilege Escalation Vulnerability","vuln_criticality":"4","vuln_threat_score":"2","vuln_zero_day":"0","vuln_create_date":"2019-02-27 00:00:00","vulnerabilities":"1","vuln_solution_status":"4","vuln_cvss_score_all":"v3:7.8","vuln_cvss_score":"0","vuln_cvss3_score":"7.8","vuln_where_type":"3","vuln_impact_type":",3,","installations":"1","products":"1","hosts":"1"},{"vuln_id":"89704","vuln_title":"cURL Insecure Permissions Privilege Escalation Vulnerability","vuln_criticality":"4","vuln_threat_score":"","vuln_zero_day":"0","vuln_create_date":"2019-06-24 00:00:00","vulnerabilities":"1","vuln_solution_status":"2","vuln_cvss_score_all":"v3:7.8","vuln_cvss_score":"0","vuln_cvss3_score":"7.8","vuln_where_type":"3","vuln_impact_type":",3,","installations":"1","products":"1","hosts":"1"},{"vuln_id":"76592","vuln_title":"Cygwin "sec_auth.cc" Privilege Escalation Vulnerability","vuln_criticality":"4","vuln_threat_score":"","vuln_zero_day":"0","vuln_create_date":"2017-04-28 00:00:00","vulnerabilities":"1","vuln_solution_status":"2","vuln_cvss_score_all":"v2:6.8","vuln_cvss_score":"6.8","vuln_cvss3_score":"0","vuln_where_type":"3","vuln_impact_type":",3,","installations":"2","products":"1","hosts":"1"},

Table 7-2 • (cont.)Configured Advisory Groups API Information

Requirement Types	Details
Received Information	SAID, Advisory Description, Criticality, Threat Score, Zero-Day, Advisory Published, Vulnerabilities, Solution Status, Installations, Products, etc.  ***Note*** *• Threat Score is available only for users with Threat Intelligence module*

A

Appendix A - Sample API Code

Sample Powershell Code to get Host Details

This Appendix section attached the sample codes to receive the Software Vulnerability Host Details as shown below:

Sample Powershell Code

```
$Site = ( "Account",     "https://csi7.secunia.com/csi/api/"    ,"username=User_Name&password=*******")
YOUR TOKEN HERE - (see How to get the Token)
$global:QueryLimit = 10000
$global:WebServiceHeader = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
$global:WebServiceHeader.Add("Content-Type", 'application/x-www-form-urlencoded')
$global:URL = $Site[1]
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$global:ErrorArray = @()

function GetData ($URL, $Retry, $Post, $Body)
{
    $result = @()
    $Count = 0
    while ($Count -lt $Retry)
    {
        try
        {
            $Count++
            if ($Post)
```

```
            {
                $result = Invoke-RestMethod -Uri $URL -Method Post -Headers $global:WebServiceHeader -
Body $Body  -WebSession $global:Session
            }
            else
            {
                $result = Invoke-RestMethod $URL -Method Get -Headers $global:WebServiceHeader -
TimeoutSec 5 -WebSession $global:Session
            }
            $result.data
            $Count = $Retry
        }
        catch
        {
            Start-Sleep -s 2
            if ($Count -eq $Retry)
            {
                $global:ErrorArray += ("Error GetData " + $URL + " " +  $_.Exception.Message + " " +
$_.Exception.ItemName+ " " + $_.Exception.Status + " " + $_.Exception.Response)
                Write-Host "Timeout Exceeded and Exhausted Retries" -ForegroundColor Red
            }
            else
            {
                Write-Host "Timeout Exceeded -- will retry in 2 sec" -ForegroundColor Yellow
            }
        }
    }
    return $result
}

function QueryData ($Post, $Token, $URL, $Body)
{
    # Get First Page of results (25 items)
    [int] $Start = 0
    [int] $Limit = 11
    [int] $CurrentTotal = -1
    $Total = 0
    $results = @()
```

```
    while ($CurrentTotal -lt $Total)
    {
        $CurrentTotal = $CurrentTotal + $Limit

        $FullURLGet = $global:URL + "?uid=" + $Token + $URL + "&start=" + [string]$Start + "&limit=" +
[string]$Limit
        $FullURLPut = $global:URL + "?uid=" + $Token + $URL
        $BodyFull =  $Body + "&start=" + [string]$Start + "&limit=" + [string]$Limit
        try
        {
            if ($Post)
            {
                $result = GetData $FullURLPut 5 $Post $BodyFull
                if ($result)
                {
                    $results = $results + $result
                }
            }
            else
            {
                $result = GetData $FullURLGet 5 $Post $Body
                if ($result.rows)
                {
                    $results = $results + $result.rows
                }
            }
            [string]$TotalString = $result.total;
            $Total = [int]$TotalString.Trim(" ");

            if ($results.Count -gt $global:QueryLimit)
            {
                break;
            }
        }
        catch
        {
            $global:ErrorArray += ("Error QueryData2 " + $result.next + " " +  $_.Exception.Message + "
" + $_.Exception.ItemName)
```

```
            return $results
        }
        $Start = $Start + $Limit
    }
    $results = $results | ? {$_}
    return $results
}

function GetUserToken ($Cred)
{
    $Data =  Invoke-WebRequest -Uri ($global:URL + "?action=manuallogin") -Body $Cred -Method Post -
Headers $global:WebServiceHeader -SessionVariable 'global:Session'
    if ($Data.StatusCode -eq 200)
    {
        $Response = ConvertFrom-Json $Data.Content
        return $Response.uid
    }
    return ""
}

$Token = GetUserToken $Site[2]
if (![string]::IsNullOrWhiteSpace($Token))
{
    $Data = QueryData $False $Token
"&action=smart_groups&which=getSmartGroupContents&smartGroupTextType=host&smartGroupId=1"
    $Count = 0
    $Data | Format-Table -Property host_name, num_insecure, num_eol, num_patched, num_installations,
nsi_device_id, score

    $Body = "device_id=1182" + "&dir=ASC" + "&eol=true" + "&insecure=true"  + "&patched=true"
    $Data2 = QueryData $True $Token "&action=hosts&which=get_host_scan_results" $Body
    $Data2.data | Format-Table -Property product_name, version, state, vuln_id, vuln_title
}
```