

# Software Vulnerability Research Release Notes

December 2023

<b>Introduction .....</b>	<b>1</b>
<b>New Features and Enhancements .....</b>	<b>2</b>
Support for CPE v2.3.....	2
<b>Resolved Issues.....</b>	<b>3</b>
<b>System Requirements .....</b>	<b>3</b>
<b>Legal Information .....</b>	<b>4</b>

## Introduction

Software Vulnerability Research provides access to verified intelligence from Secunia Research, covering all applications and systems across all platforms. Prioritization is driven by threat intelligence, workflows, tickets and alerts, and describes the steps to mitigate the risk of costly breaches. You stay in control and hackers stay out. For more information, see <https://www.flexera.com/products/operations/software-vulnerability-research.html>

# New Features and Enhancements

Software Vulnerability Research includes the following new features and enhancements:

- [Support for CPE v2.3](#)

## Support for CPE v2.3

CPE stands for Common Platform Enumeration. CPE naming specifications define standardized methods for assigning names to IT product classes. With this update, SVR will now support CPE v2.3 for naming the software products. To view the CPE v2.3 product naming, click on any **SAID > CPE Exists**, **Click for Details** link a popup appears with the CPE 2.3 details.

Effective December 15, 2023, NVD will retire the CPE v2.2 legacy feed. Consequently, current products in SVR will be visible in both CPE v2.2 and CPE v2.3 naming formats during this transitional period. However, it's important to note that any new products added to SVR in the future will be displayed in the CPE v2.3 naming format, and the CPE v2.2 format only if available.

CPE 2.3 details - IBM App Connect Enterprise 11.x		
CPE Name ID	CPE Name	Modification date
4CB0BB70-45F3-4ABA-8B57-6A3B1BE27AE8	cpe:2.3:a:ibm:app_connect:11.0.0.2:*****	2021-04-22
81E952AB-E310-4FA2-8200-5D7710F6F2FD	cpe:2.3:a:ibm:app_connect:11.0.0.1:*****	2021-04-22
D341AC0B-F7CA-4A3F-86C1-8946FC34A395	cpe:2.3:a:ibm:app_connect:11.0.0.0:*****	2021-04-22
CPE 2.2 details - IBM App Connect Enterprise 11.x		
NVD ID	CPE Name	Modification date
1339520	cpe:/a:ibm:app_connect_enterprise:11.0.0.8	2023-02-24
1339521	cpe:/a:ibm:app_connect_enterprise:11.0.0.19	2023-02-24
898710	cpe:/a:ibm:app_connect:11.0.0.0	2021-04-22
898711	cpe:/a:ibm:app_connect:11.0.0.2	2021-04-22
898712	cpe:/a:ibm:app_connect:11.0.0.1	2021-04-22
1503760	cpe:/a:ibm:app_connect_enterprise:11.0.0.1	2023-10-30
1503761	cpe:/a:ibm:app_connect_enterprise:11.0.0.23	2023-10-30
Back		

## REST API Enhancement

The following new REST API has been added for the Products:

REST API	Description
<a href="#">/api/cpe23-products/</a>	This new API is introduced in this update. This API will return the entire list of CPEs v2.3 and when available, its associated product in SVR.

The following existing REST API have extended support:

REST API	Description
<b>/api/advisories/</b>	This API now returns a new property named cpes23. This new property contains the products in the CPE v2.3 naming format that are affected by the selected advisory.
<b>/api/product-releases/</b>	This API now returns a new property named cpes23. For the selected product, when available, the cpes23 property contains the CPE v2.3 naming format of the product.

## Resolved Issues

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

Issue	Description
<b>IOK-1077616</b>	macOS Sonoma is not detecting in the SVR agent.
<b>IOK-1072970</b>	The Microsoft Silverlight EOL product is showing as Secure.
<b>IOK-1075930</b>	In the Suggest a Software > Single software tab, Software version property should be mandatory.

## System Requirements

Software Vulnerability Research's user interface will resize and adapt when being used on different devices. You can access the system from anywhere using any device, such as a smart phone or tablet, running Microsoft Edge, Chrome, Opera, Firefox, Safari and mobile browsers with an Internet connection capable of connecting to <https://app.flexerasoftware.com>.

# Legal Information

## Copyright Notice

Copyright © 2023 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/legal/intellectual-property.html>. 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.