

# Software Vulnerability Research Release Notes

May 2023

<b>Introduction .....</b>	<b>1</b>
<b>New Features and Enhancements .....</b>	<b>2</b>
Technology Stack Upgrade.....	2
Rejected Advisories Renamed to Rejection Advisories .....	2
<b>System Requirements .....</b>	<b>2</b>
<b>Legal Information .....</b>	<b>3</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

This Software Vulnerability Research update includes the following:

- [Technology Stack Upgrade](#)
- [Rejected Advisories Renamed to Rejection Advisories](#)

## Technology Stack Upgrade

This release includes significant upgrades to the underlying software frameworks and components of SVR. This technology stack upgrade results in a more secure, improved, and stable version of the SVR.

## Rejected Advisories Renamed to Rejection Advisories

In the Research > Advisory Database view, the Rejected Advisories are now renamed to Rejection Advisories.

SAID	Release date	Modified date	Title	Criticality	Zero Day	Solution status	Where	CVSS Score	Threat score	Type
SA116004	2023-05-18	2023-05-18	Ubuntu update for cups-filters	Low	No	Vendor Patched	From local network	8.8 v3	15	Secunia Advisory
SA116033	2023-05-18	2023-05-18	Cisco Identity Services Engine (ISE) Multiple Vulnerabilities	Low	No	Vendor Patched	From local network	3.5 v3	0	Secunia Advisory
SA116041	2023-05-18	2023-05-18	Cisco DNA Center API Multiple Vulnerabilities	Low	No	Vendor Patched	From local network	4.6 v3	0	Secunia Advisory
SA116051	2023-05-18	2023-05-18	Cisco Identity Services Engine (ISE) Multiple Information Disclosure Vulnerabilities	Low	No	Vendor Patched	From local network	3.5 v3	0	Secunia Advisory
SA116077	2023-05-18	2023-05-18	NetApp ONTAP PHP Denial of Service Vulnerability	Low	No	Vendor Patched	From local network	6.5 v3	3	Secunia Advisory
SA116080	2023-05-18	2023-05-18	Veritas InfoScale Log4j Multiple Vulnerabilities	Low	No	Vendor Patched	From remote	9.8 v3	99	Secunia Advisory
SA116008	2023-05-18	2023-05-18	IBM WebSphere Service Registry and Repository Studio IBM Java Multiple Vulnerabilities	Low	No	Vendor Patched	From local network	5.4 v3	7	Secunia Advisory
SA116037	2023-05-18	2023-05-18	Cisco Identity Services Engine (ISE) Rejection Notice	Low	No	None	None	-	0	Rejection Advisory
SA116079	2023-05-18	2023-05-18	SUSE ovmf Rejection Notice	Low	No	None	None	-	0	Rejection Advisory
SA116074	2023-05-18	2023-05-18	SUSE update for java-1_8_0-openjdk	Low	No	Vendor Patched	From remote	7.4 v3	23	Secunia Advisory
SA116055	2023-05-18	2023-05-18	Ubuntu update for linux	Low	No	Vendor Patched	Local system	7.8 v3	19	Secunia Advisory
SA116048	2023-05-18	2023-05-18	Cisco Identity Services Engine (ISE) Rejection Notice	Low	No	None	None	-	0	Rejection Advisory
SA116065	2023-05-18	2023-05-18	Red Hat update for apr-util	Low	No	Vendor Patched	From remote	9.8 v3	17	Secunia Advisory

## 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.