

Software Vulnerability Manager (Cloud Edition) Release Notes

May 2023

Introduction	1
New Features and Enhancements	1
Hyperlinks in Advisory Details Window	2
Smart Groups Compilation Improvements.....	2
Reference: Latest Binary Versions.....	3
Community Blogs.....	3
Product Feedback	3
Legal Information	4

Introduction

Flexera's Software Vulnerability Manager is a software vulnerability and patch management solution that facilitates a customized patch management process. It combines vulnerability and threat intelligence, end point assessment, and patch creation and publishing enable an informed and rapid patch management.

Software Vulnerability Manager can assess software vulnerabilities for both Microsoft and non-Microsoft (third-party) product vulnerabilities covering Microsoft Windows, macOS, and Red Hat Enterprise Linux. The results of this assessment are connected to our vulnerability and threat intelligence to allow for effective prioritization. Finally, third party patches may be created and published to remediate endpoints using Microsoft® WSUS (often in conjunction with System Center Configuration Manager), via Microsoft® Intune, VMware® Workspace One, or BigFix.

New Features and Enhancements

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

- [Hyperlinks in Advisory Details Window](#)
- [Smart Groups Compilation Improvements](#)
- [Reference: Latest Binary Versions](#)



Note • To see the following new features and enhancements in your Software Vulnerability Manager (Cloud Edition) interface, you must refresh your browser's cache (press Ctrl+F5).

Hyperlinks in Advisory Details Window

In the Advisory details window, **CVE Reference(s)** and **Original Advisory** links are now clickable. By clicking on the **CVE Reference(s)** link it navigates to cve.mitre.org website for cybersecurity vulnerabilities information.

Clicking **Original Advisory** links navigates to external Websites for additional details.

Amazon Corretto Multiple Vulnerabilities

Secunia Advisory ID: SA113414

Creation Date: 2023-01-18

Criticality - Moderately critical

Threat Score: 7

Impact: Manipulation of data
DoS

Where: From remote

Solution Status: Vendor Patched

Secunia CVSS3 Scores: Base: 5.3, Overall: 4.6 CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:U/RL:O/RC:C

CVE Reference(s): [CVE-2023-21830](#), [CVE-2023-21835](#), [CVE-2023-21843](#)

Affected Software

Amazon Corretto 11.x
Amazon Corretto 8.x

Secunia Advisory Details

Multiple vulnerabilities have been reported in Amazon Corretto, which can be exploited by malicious people to manipulate certain data and cause a DoS (Denial of Service).

For more information:
SA113442 (#1 through #3)

The vulnerabilities are reported in versions prior to 11.0.18.10.1 and prior to 8.362.08.1.

Solution

Update to version 11.0.18.10.1 or version 8.362.08.1.

Original Advisory

<https://raw.githubusercontent.com/corretto/corretto-8/develop/CHANGELOG.md>
<https://raw.githubusercontent.com/corretto/corretto-11/develop/CHANGELOG.md>

Other References

SA113442

Close

Smart Groups Compilation Improvements

Check boxes have been added in **Create & Edit** grid of Host Smart Groups/Product Smart Groups/Advisory Smart Groups to support complication of multiple smart groups at once. By clicking check boxes by multiple smart groups, you can initiate compilation of one or more smart groups at a time.

Name	Description	Business Impact	Completion	Data Last Compiled	Unique Products	Installations	Hosts	Modified Date
All Products	Smart Group conta...		Complete	15th May, 2023 17...	517	2486	19	11th Feb, 2020 12:1
End-Of-Life Pr...	Smart Group conta...		Complete	15th May, 2023 17...	51	141	15	11th Feb, 2020 12:1
Insecure Produ...	Smart Group conta...		Complete	15th May, 2023 17...	119	310	19	11th Feb, 2020 12:1
Patched Produ...	Smart Group conta...		Complete	15th May, 2023 17...	384	2035	19	11th Feb, 2020 12:1

Reference: Latest Binary Versions

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.0.24 (no change)
- Single Host Agent v7.6.0.24 (no change)
- SVM Daemon v7.6.0.24 (no change)
- SVM System Center Plugin v7.6.0.24 (no change)
- SVM Patch Publisher v7.9.906 (to download, [click here](#)) (no change)
- SVM Cloud Client Toolkit v5.0.561 (to download, [click here](#)) (no change)

This toolkit contains offline utilities such as the Multi-partition Reporting Tool, WSUS Management Tool and Client Data Tool which add value to SVM. This toolkit does not consist of Patch Daemon. This toolkit is for SVM Cloud edition only.



Note • The [Flexera SVM Patch Configuration](#) will be deprecated in the future; therefore, you are encouraged to migrate to the new SVM Patch Publisher tool.

Community Blogs

Please subscribe to latest posts about Software Vulnerability Manager by going to <https://community.flexera.com/t5/Software-Vulnerability/bg-p/SoftwareVulnerabilityManagementblog> and clicking on subscribe.

Please subscribe to latest release announcements concerning Software Vulnerability Manager by going to <https://community.flexera.com/t5/Software-Vulnerability/bg-p/Software-Vulnerability-Release-blog> and clicking on subscribe.

Product Feedback

Have a suggestion for how we can improve this product? Please share your feedback with the product team by visiting the Software Vulnerability Manager Forum in the Flexera Community:

<https://community.flexera.com/t5/Software-Vulnerability/bd-p/SVM-Discussion>

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.