OpenText™ Application Security Aviator for Vulnerability Remediation

Release Notes

Version : 26.2

PDF Generated on : April 9, 2026

© Copyright 2026 Open Text

Table of Contents

1. Release Notes

This document provides the new features, installation and upgrade notes, known issues, and workarounds that apply to release 26.2 of OpenText™ Application Security Aviator for Vulnerability Remediation .

This information is not available elsewhere in the product documentation. The user guides for this product are available on the Product Documentation website: https://www.microfocus.com/documentation/fortify-static-code/

1.1. Fortify product name changes

OpenText is in the process of changing the following product names:

Previous name	New name
Fortify Static Code Analyzer	OpenText™ Static Application Security Testing (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Dynamic Application Security Testing (OpenText DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	OpenText™ Core Software Composition Analysis (OpenText Core SCA)
Fortify Applications and Tools	OpenText™ Application Security Tools

The product names have changed on product splash pages, mastheads, login pages, and other places where the product is identified. The name changes are intended to clarify product functionality and to better align the Fortify Software products with OpenText. In some cases, such as on the documentation title page, the old name might temporarily be included in parenthesis. You can expect to see more changes in future product releases.

1.2. New features

Language support

- All categories for Apex, PHP, C/C++, ABAP, and Scala are now supported with automatic suppression.

New features/updates

- OpenText™ Core SAST Aviator has now been renamed to OpenText™ Application Security Aviator for Vulnerability Remediation.
- OpenText Application Security Aviator for Vulnerability Remediation supports `skip-if-exceeding-quota` and `test-exceeding-quota` options for both individual and bulk audits, allowing users to prevent automatic consumption of quota on application versions that have more open issues than available quota. When an application version exceeds quota, the audit is skipped with a detailed message showing open issue count, available quota, and top 10 SAST categories, enabling users to manually triage issues before auditing for optimal quota utilization.
- When available quota is insufficient to audit all open issues, OpenText Application Security Aviator for Vulnerability Remediation prioritizes issues based on their folder hierarchy (typically Critical → High → Medium → Low) as defined in the FPR file. Users can customize the default prioritization order using command-line option or configuration to align with the required priority, ensuring the most critical issues are audited first when quota is limited.
- Introduces a configurable mapping mode that allows OpenText Application Security Aviator for Vulnerability Remediation applications to be created for each OpenText™ Application Security (Fortify Software Security Center) application or for each application version. Enables quota tracking and auditing for users who use application versions to represent distinct components.
- New options allow applying remediations from the latest OpenText Application Security Aviator for Vulnerability Remediation run, across all open issues for an application version, or within a defined time window (`--latest` , `--all` , `--since`).

Installation and upgrade notes

- fcli v3.17.x or later