

OpenText™ Core SAST Aviator

Release Notes

Version : 25.3.0

PDF Generated on : 23/07/2025

Table of Contents

- 1. Release Notes 3
 - 1.1. Fortify product name changes 4
 - 1.2. New features 5

1. Release Notes

This document provides the new features, installation and upgrade notes, known issues, and workarounds that apply to release 25.3.0 of OpenText™ Core SAST Aviator.

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 .NET are now supported with automatic suppression, except for Code Correctness, Dead Code, Poor Error Handling, and Unsafe Native Invoke.

Features/updates

- Support to view the real-time health status and uptime metrics of SAST Aviator at [Status Page - Fortify on Demand](#).
- The email ID associated with managing user tokens is the user's email ID, which is other than the administrator's email ID.
- The language used in the LLM response is much clearer, polite, and solution-oriented.
- Support to view the specific remediation steps or suggestions for each identified vulnerability based on the vulnerability type, programming language, and code snippet in an XML file. The remediation XML file is uploaded with the audited FPR to the Fortify Software Security Center application version.

Installation and upgrade notes

- v3.8.0 or later



© Copyright 2025 Open Text
For more info, visit <https://docs.microfocus.com>
