OpenText™ Core Application Security Remediation Extension for Visual Studio Code Version 25.2

Release Notes

Document Release Date: May 2025
Software Release Date: May 2025

This is the first release of OpenText™ Core Application Security Remediation Extension for Visual Studio Code.

The user guide for this product is available on the Product Documentation website:

https://www.microfocus.com/documentation/fortify-on-demand/

UPDATES TO THIS DOCUMENT

Date	Addition and/or change
5/22/2025	First release.

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.

Accessing Documentation

The documentation set contains installation, deployment, and user guides. In addition, you will find release notes that describe last-minute updates. You can access the latest HTML and/or PDF versions of the documents for this release from the Product Documentation website:

https://www.microfocus.com/documentation/fortify-on-demand/

If you have trouble accessing our documentation, please contact Customer Support.

About OpenText™ Core Application Security Remediation Extension for Visual Studio Code

The OpenText™ Core Application Security Remediation Extension for Visual Studio Code enables you to view and audit issues directly from an application version release in Core Application Security. The extension provides an interface to view the scan results with code navigation, explanations of the vulnerabilities, and recommendations on how to fix them. The extension also provides the ability to audit the issues and add comments, which directly sync with the Core Application Security portal.

DEFINITIONS

Deprecation

When a product feature or integration is deprecated, OpenText no longer accepts enhancement requests for the feature but does respond to critical or security defects. OpenText will continue to support the usage of a deprecated feature or integration. If applicable, the feature is turned off by default, but customers can re-enable it. OpenText will stop supporting the feature or integration on the removal date or in the removal release.

Removal

When a product feature or integration is removed, OpenText no longer accepts or responds to critical or security defects. If the feature is a function, coded in the product, all code is removed, and the feature no longer functions in the product. If the feature is an external system or integration, the ability to integrate or be used by the product is removed and OpenText no longer supports its use or ability to function.

SUPPORT

If you have questions or comments about using this product, contact Customer Support using the following option.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account: https://www.microfocus.com/support.

LEGAL NOTICES

Copyright 2025 Open Text

WARRANTY

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.