OpenText™ Core Application Security

Release Notes

Version : 26.1

PDF Generated on : January 8, 2026

Table of Contents

1. Release Notes

This document provides the new features, installation and upgrade notes, known issues, and workarounds that apply to release 26.1.0 of OpenText™ Core Application Security (Fortify on Demand).

This information is not available elsewhere in the product documentation. The user guides for this product are available on the Product Documentation website: OpenText Core Application Security (Fortify on Demand) - Documentation | Micro Focus

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
Fortify Aviator	OpenText™ Core SAST Aviator (SAST Aviator)

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. Engine and rulepack updates

OpenText Core Application Security 26.1.0 includes the following engine and rulepack updates.

Fortify Software Security Content 25.4

OpenText Core Application Security will implement Fortify Software Security Content 25.4 from Fortify Security Research (SSR) after the 26.1.0 release. *For more information, see Fortify Software Security Content 25.4*.

OpenText Static Application Security Test 25.4

OpenText Core Application Security will implement OpenText Static Application Security Testing (Fortify Static Code Analyzer) version 25.4 for source code scanning after the 26.1.0 release.

1.3. New features

SARIF import support

Core Application Security now supports importing, storing, and displaying SARIF files, allowing a unified view of third-party SAST results. *For more information, see "Importing an On-Premises Scan" in the Core Application Security User Guide.*

SPDX SBOMs from Debricked scan results are available for download

Core Application Security now supports exposing SPDX SBOMs to customers, in addition to the existing CycloneDX format. To enable this capability, the **Download SBOM** option on the **Your Scans**, **Application Scans**, and **Release Scans** pages has been updated to offer two formats, **CycloneDX** and **SPDX**. *For more information, see "Viewing All Scans", "Viewing Application Scans" and "Viewing Release Scans" in the Core Application Security User Guide.*

Support for adding attributes to scans

Customers can now add custom attributes (e.g., Git commit ID, build ID) to scans, making it easier to trace results to specific code changes or deployments and to filter or report on scans in CI/CD workflows. *For more information, see "Adding an Attribute" in the Core Application Security User Guide.*

Dashboard filtering by custom attributes

FoD customers can now filter dashboard charts using custom attributes defined in their tenant across multiple data types. *For more information, see "Magellan Dashboards" in the Core Application Security User Guide.*

Support for OWASP ASVS 5.0

Core Application Security now fully supports OWASP ASVS 5.0, including new report templates, issues export columns, grouping and filter options, and selection in security policies.

Remediation grace period information available on Issues page

Developers can now view the remaining remediation grace period for open issues when a grace period is defined in the application policy. This enhancement enables better prioritization and timely remediation before a policy failure occurs. To support this capability, a new **Remediation Grace Period** field has been added to the **Release Issues** and **Application Issues** pages. *For more information, see "Viewing Application Issues" and "Viewing Release Issues" in the Core Application Security User Guide.*

Support for setting auditor status during issue suppression through the audit filter

The Audit Templates configuration page now includes an enhancement that displays a secondary drop-down list when **Suppress** is selected as the filter action. This drop-down allows users to specify the **Auditor Status** that is automatically applied when an issue is suppressed. *For more information, see "Creating a Global Audit Template" and "Creating an Application Audit Template" in the Core Application Security User Guide.*

Ability to create audit filters for open-source issues based on file location

Audit filters now support file-location based filtering for open-source issues. To enable this capability, the *File Location* attribute has been added to the Open Source scan type. *For more information, see "Creating a Global Audit Template" and "Creating an Application Audit Template" in the Core Application Security User Guide.*

API updates

The following updates have been made to the OpenText™ Core Application Security API:

- SARIF import: A new API endpoint, `PUT /api/v3/releases/{releaseId}/static-scans/import-sarif`, enables importing SARIF files for applications and releases.
- The endpoint `GET /api/v3/applications/{applicationId}/users` now includes `accessMethod` details for each user.
- The endpoint `GET /api/v3/source-scans/{scanId}/sbom` is enhanced to support both **CycloneDX** and **SPDX** SBOM formats.
- The endpoint `GET /api/v3/applications/{applicationId}/users` now includes the email ID, role name and role ID.
- Postman API scan setup: The endpoint `GET /dynamic-scans/scan-setup and PATCH /dynamic-scans/scan-setup/manifest` now return all uploaded files with the Postman collection, supporting multiple Postman file types.
- Vulnerability endpoints: The endpoint `GET /vulnerabilities/{vulnId}/all-data and /vulnerabilities/{vulnId}/details` now include the nullable **remainingRemediationGracePeriodDays** field.

1.4. Bug fixes

The following issues are fixed in OpenText Core Application Security 26.1.0.

- Previously, release owners received system-generated emails when a scan was completed. This email notification is no longer sent upon scan completion.

1.5. Known Issues

Issues with PDF outputs

Description

The customer-facing PDF documents of Core Application Security contains cross-reference links that do not navigate to the intended section or page. Users relying on these links to quickly access referenced content may need to locate the information in the document manually.

Workaround

Use the search feature in the PDF viewer to locate the referenced section manually.

Status

The issue is under investigation.

opentext™

For more info, visit https://docs.microfocus.com