OpenText™ Core Application Security

Release Notes

Version : 26.2

PDF Generated on : April 16, 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 26.2.0 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 details

OpenText Core Application Security 26.2.0 includes the following engine and rulepack versions:

- **Fortify Software Security Content 26.1.0:**
  OpenText Core Application Security implements Fortify Software Security Content 26.1. For more information, see Fortify Software Security Content 26.1.
- **OpenText Static Application Security Test 26.1.0:**
  OpenText Core Application Security implements OpenText SAST (Fortify Static Code Analyzer) version 26.1.

1.3. New features

AI-powered SAST

Core Application Security now includes AI-powered scanning support for 12 additional programming languages, enabled by our next-generation SAST architecture. This enhanced architecture significantly accelerates the onboarding of new languages, allowing future language support to be delivered faster and more efficiently. To enable this capability, a new setting, Enable AI-Powered SAST, is available under Administration → Settings → SAST.

For more information, see Configuring SAST in the Core Application Security User Guide.

Note
This feature has been released but is not currently available. It will be enabled at a later date.

Remediation dashboard enhancements

Core Application Security 26.2 introduces the following charts to new remediation dashboard:

- Review coverage by severity - Shows the percentage of identified security issues reviewed across each severity level.
- Remediation coverage by severity - Shows the percentage of issues remediated by severity level, highlighting how effectively higher-risk vulnerabilities are being addressed.
- Issue remediation trend - Shows monthly remediation trends by severity to support planning, prioritization, and resource allocation.
- Frequently reopened issues - Shows a ranked list of security issue categories that are most frequently reopened, helping identify areas requiring deeper root-cause analysis or process improvements.
- Review coverage by scan type - Shows the percentage of remediated issues based on scan type, indicating remediation effectiveness across various security testing approaches.
- Remediation coverage by scan type - Shows the percentage of remediated issues based on the type of scan.

- SAST Aviator adoption - Shows a visual summary of SAST Aviator adoption across all managed applications.
- Mean time to remediate - This view highlights the improvement in remediation timelines compared to the previous year and clearly shows the year-over-year (YoY) change.
- Mean time to remediate by severity - Shows the average remediation time broken down by severity level, demonstrating how effectively higher-risk issues are prioritized.
- Issue reopened rate - Shows the current percentage of reopened issues, including exact counts.
- SAST Aviator return on investment (ROI) - Shows estimated financial savings and time efficiencies achieved through SAST Aviator, highlighting the business value of early vulnerability detection and remedia.

For more information, see New Dashboards in the Core Application Security User Guide.

2FA-secured DAST scanning

Core Application Security now supports dynamic scanning of applications protected by Two-Factor Authentication (2FA). This enhancement enables secure assessment of applications that require multi-factor authentication while maintaining strong access controls. To support this capability, the DAST setup form has been updated with additional configuration fields, allowing teams to provide the necessary authentication details for 2FA-enabled applications and run dynamic scans successfully.

For more information, see Configuring a Dynamic Scan in the Core Application Security User Guide.

SCIM integration support

Core Application Security 26.2 introduces a new SCIM Integration feature that enables automated provisioning of users and groups between a customer's Identity Provider (IdP) and their tenant, in alignment with the SCIM 2.0 standard. To support this capability, a new SCIM Integration tab has been added under Administration → User Management in the tenant portal. This dedicated interface provides centralized configuration and management of SCIM-based provisioning.

For more information, see Configuring System for Cross-domain Identity Management (SCIM) in the Core Application Security User Guide.

SCIM integration with Single Sign-On (SSO)

In addition, SCIM provisioning can now be enabled directly through Single Sign-On (SSO). By enabling SCIM from the SSO configuration, organizations can streamline identity authentication and lifecycle management within a single, centralized workflow.

For more information, see Configuring SSO in OpenText Core Application Security in the Core Application Security User Guide.

DAST: Site Tree availability for manual scans

Core Application Security now provides access to the site trees captured during dynamic manual web application scans. This capability enables greater visibility into the scanned application structure and supports more effective analysis and review. Site tree file is available for download directly from the Scans page.

For more information, see Viewing Release Scans in the Core Application Security User Guide.

Grouped manual and automated DAST results

Core Application Security now allows customers to categorize Dynamic+ findings by whether they were discovered through manual assessments or automated scans, offering improved clarity into how vulnerabilities are detected.
For more information, see Viewing Release Scans in the Core Application Security User Guide.

Security standards updates

Core Application Security now provides full support for the latest industry security standards, enhancing reporting, analysis, and policy management across the platform.
The following standards are now fully supported:

- DISA STIG 6.4
- CWE TOP 25 2025
- OWASP TOP 10 2025
- OWASP Top 10 for LLM Applications 2025

API key role for user management

Core Application Security 26.2 introduces a new API key role, Manage Users, which enables API-based management of users and user groups without requiring elevated permissions. This new role allows you to automate and integrate user management

workflows more securely and efficiently while maintaining appropriate access controls.

For more information, see API Key Roles in the Core Application Security User Guide.

System notification changes

Starting with Core Application Security 26.2, security leads automatically receive email notifications whenever tenant Single Sign-On (SSO) settings are modified. This enhancement increases visibility into identity-related configuration changes and helps ensure timely awareness and governance of authentication settings.

Provisioning developer entitlements

Core Application Security now includes enhancements to the Entitlements page to support developer-based licensing. Tenant administrators can configure developer-based entitlements during tenant setup and manage them alongside application-based licensing. All entitlement types are now displayed in a single, consolidated interface, making it easier to view totals, track consumption, monitor availability, and review expiration details. These enhancements simplify entitlement management and provide greater transparency across all licensing models.

For more information, see Viewing Entitlements in the Core Application Security User Guide.

Expanded support for CycloneDX versions

Core Application Security now extends its existing CycloneDX SBOM import capability to include JSON files conforming to the CycloneDX 1.7 specification. Previously supported versions remain unchanged, with this update broadening compatibility to the latest CycloneDX standard.

For more information, see Importing a Software Bill of Materials in the Core Application Security User Guide.

Enhanced attribute configuration

You can now enable Required and Editable only by Security Leads together when configuring attributes. When both options are selected, the system now requires a default value to ensure the attribute is populated properly during entity creation. For 'Picklist' attributes, this default must be selected from the available list values.

For more information, see Adding an Attribute in the Core Application Security User Guide.

MAST+ support for additional credential fields

MAST+ setup now supports more advanced authentication workflows. You can add up to three additional credential fields for form authentication during MAST+ scans.

For more information, see Configuring a Mobile Scan in the Core Application Security User Guide.

API updates

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

- The vulnerability bulk edit endpoint has been enhanced to support broader update scenarios:
  - `POST /api/v3/releases/{releaseId}/vulnerabilities/bulk-edit`

  This endpoint now includes an optional boolean parameter, includeAllVulnerabilities, which allows bulk updates to be applied to all vulnerabilities associated with a release, without requiring individual vulnerability or issue IDs. This simplifies large-scale remediation updates and automation workflows.

- The following attribute endpoints now support configurations where both Required and Restricted (editable only by Security Leads) can be enabled simultaneously:
  - `POST /api/v3/attributes`
  - `PUT /api/v3/attributes/{attributeId}`

  This enhancement ensures parity with UI-based attribute configuration and enforces consistent data governance during entity creation.

- The following static scan endpoints have been enhanced to support AI-Powered SAST:
  - `POST /api/v3/releases/{releaseId}/static-scans/start-scan`
  - `POST /api/v3/releases/{releaseId}/static-scans/start-scan-with-defaults`
  - `POST /api/v3/releases/{releaseId}/static-scans/start-scan-advanced`

  These updates allow customers to integrate AI-powered static analysis seamlessly into automated pipelines.

- New reporting endpoints have been added to support automated data export and processing, eliminating the need for manual actions in the portal:

    - GET /api/v3/reports/dataexports/templates - Retrieves available data export templates.
    - POST /api/v3/reports/dataexports - Initiates a new data export.
    - GET /api/v3/reports/dataexports/{dataExportId} - Retrieves the status and details of a specific data export

- As part of developer-based license capabilities, the following endpoints now support capturing the developer based license information.:
    - `GET /api/v3/tenant-entitlements`
    - `GET /api/v3/tenant-open-source-entitlements`

1.4. 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.

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