OpenText™ Core Application Security

Notas de la versión (26.1.0)

Version : 26.1

PDF Generated on : February 12, 2026

© Copyright 2026 Open Text

Table of Contents

1. Notas de la versión (26.1.0)

Este documento proporciona las nuevas características, notas de instalación y actualización, problemas conocidos y soluciones alternativas que se aplican a la versión 26.1.0 de OpenText™ Core Application Security (Fortify on Demand).
Esta información no está disponible en ninguna otra parte de la documentación del producto. Las guías de usuario de este producto están disponibles en el sitio web de Documentación del producto:
OpenText Core Application Security (Fortify on Demand) - Documentación | Micro Focus

1.1. Cambios de nombre de producto de Fortify

OpenText está en proceso de cambiar los siguientes nombres de productos:

Nombre anterior	Nuevo nombre
Fortify Static Code Analyzer	Pruebas de seguridad de las aplicaciones estáticas OpenText™ (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	Pruebas de seguridad de las aplicaciones dinámicas OpenText™ (OpenText DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	Análisis de composición de software OpenText™ Core (OpenText Core SCA)
Fortify Applications and Tools	OpenText™ Application Security Tools
Fortify Aviator	OpenText™ Core SAST Aviator (SAST Aviator)

Los nombres de los productos han cambiado en las páginas de presentación, encabezados, páginas de inicio de sesión y otros lugares donde se identifica el producto. Los cambios de nombre tienen como objetivo aclarar la funcionalidad del producto y alinear mejor los productos de Fortify Software con OpenText. En algunos casos, como en la página de título de la documentación, el nombre antiguo podría incluirse temporalmente entre paréntesis. Es posible que veamos más cambios en futuros lanzamientos de productos.

1.2. Actualizaciones del motor y del paquete de reglas

OpenText Core Application Security 26.1.0 incluye las siguientes actualizaciones del motor y del paquete de reglas.

Fortify Software Security Content 25.4

OpenText Core Application Security implementará Fortify Software Security Content 25.4 de Fortify Security Research (SSR) después de la versión 26.1.0. *Para obtener más información, consulte Fortify Software Security Content 25.4*.

Pruebas de seguridad de las aplicaciones estáticas OpenText 25.4

OpenText Core Application Security implementará OpenText Static Application Security Testing (Fortify Static Code Analyzer) versión 25.4 para el análisis de código fuente después de la versión 26.1.0.

1.3. Nuevas características

Soporte técnico para importar SARIF

Core Application Security ahora admite la importación, el almacenamiento y la visualización de archivos SARIF, lo que permite una vista unificada de los resultados SAST de terceros. *Para obtener más información, consulte "Importar un análisis local" en la Guía del usuario de Core Application Security.*

Los SBOM SPDX de los resultados del análisis de Debricked están disponibles para descargar

Core Application Security ahora admite la exposición de SBOM SPDX a los clientes, además del formato CycloneDX existente. Para habilitar esta capacidad, la opción **Descargar SBOM** en las páginas **Sus análisis**, **Análisis de la aplicación** y **Análisis de versión** se han actualizado para ofrecer dos formatos, **CycloneDX** y **SPDX**. *Para obtener más información, consulte "Visualización de todos los análisis", "Visualización de análisis de la aplicación" y "Visualización de análisis de versión" en la guía del usuario de Core Application Security.*

Soporte técnico para agregar atributos a los análisis

Los clientes ahora pueden agregar atributos personalizados (por ejemplo, Id. de confirmación de Git, Id. de compilación) a los análisis, lo que hace más fácil hacer el seguimiento de los resultados hasta cambios de código o implementaciones específicos y filtrar o informar sobre los análisis en flujos de trabajo de CI/CD. *Para obtener más información, consulte "Adición de un atributo" en la guía del usuario de Core Application Security.*

Filtrado del panel de control por atributos personalizados

Los clientes de FoD ahora pueden filtrar los gráficos del panel utilizando atributos personalizados definidos en su inquilino en múltiples tipos de datos. *Para obtener más información, consulte "Paneles de Magellan" en la Guía del usuario de Core Application Security.*

Soporte técnico para OWASP ASVS 5.0

Core Application Security ahora es totalmente compatible con OWASP ASVS 5.0, incluidas nuevas plantillas de informes, columnas de exportación de problemas, opciones de agrupación y filtrado, y la selección en directivas de seguridad.

Información sobre el periodo de gracia de corrección disponible en la página Problemas

Los desarrolladores ahora pueden ver el periodo de gracia de corrección restante para problemas abiertos cuando se define un período de gracia en la política de la aplicación. Esta mejora permite una mejor priorización y una corrección oportuna antes de que se produzca un error en la política. Para respaldar esta capacidad, se ha agregado un nuevo **Periodo de gracia de corrección** a las páginas **Problemas de versión** y **Problemas de la aplicación**. *Para obtener más información, consulte "Visualización de los problemas de la aplicación" y "Visualización de los problemas de versión" en la guía del usuario de Core Application Security.*

Soporte técnico para establecer el estado del auditor durante la supresión de problemas a través del filtro de auditoría

La página de configuración de Plantillas de auditoría ahora incluye una mejora que muestra una lista desplegable secundaria cuando **Suprimir** se selecciona como acción de filtro. Este menú desplegable permite a los usuarios especificar el **Estado del auditor** que se aplica automáticamente cuando se ha suprimido un problema. *Para obtener más información, consulte "Creación de una plantilla de auditoría global" y "Creación de una plantilla de auditoría de aplicaciones" en la guía del usuario de Core Application Security.*

Capacidad de crear filtros de auditoría para problemas de código abierto según la ubicación de archivo

Los filtros de auditoría ahora admiten el filtrado basado en la ubicación de archivos para problemas de código abierto. Para habilitar esta capacidad, se ha agregado el atributo *Ubicación de archivo* al tipo de análisis de código abierto. *Para obtener más información, consulte "Creación de una plantilla de auditoría global" y "Creación de una plantilla de auditoría de aplicaciones" en la guía del usuario de Core Application Security.*

Actualizaciones de la API

Se introdujeron las siguientes actualizaciones en la API de OpenText™ Core Application Security:

- Importación SARIF: un nuevo extremo de API, `PUT /api/v3/releases/{releaseId}/static-scans/import-sarif`, permite importar archivos SARIF para aplicaciones y versiones.
- El extremo `GET /api/v3/applications/{applicationId}/users` ahora incluye detalles de `accessMethod` para cada usuario.
- El extremo `GET /api/v3/source-scans/{scanId}/sbom` se ha mejorado para que sea compatible con los dos formatos de SBOM **CycloneDX** y **SPDX**.
- El extremo `GET /api/v3/applications/{applicationId}/users` ahora incluye el Id. de correo electrónico, el nombre del rol y el Id. de rol.
- Configuración del análisis de API de Postman: El extremo `GET /dynamic-scans/scan-setup and PATCH /dynamic-scans/scan-setup/manifest` ahora devuelve todos los archivos cargados con la colección Postman, siendo compatible con múltiples tipos de archivos Postman.
- Extremos de vulnerabilidad: El extremo `GET /vulnerabilities/{vulnId}/all-data and /vulnerabilities/{vulnId}/details` ahora incluye el campo anulable **remainingRemediationGracePeriodDays**.

1.4. Corrección de errores

Los siguientes problemas se han solucionado en OpenText Core Application Security 26.1.0.

- Anteriormente, los propietarios de las versiones recibían correos electrónicos generados por el sistema cuando se completaba un análisis. Esta notificación por correo electrónico ya no se envía una vez completado el análisis.

1.5. Problemas conocidos

Problemas con las salidas de PDF

Descripción

Los documentos PDF de Core Application Security que ven los clientes contienen vínculos de referencia cruzada que no dirigen a la sección o página prevista. Los usuarios que dependen de estos vínculos para acceder rápidamente al contenido referenciado pueden necesitar localizar la información en el documento manualmente.

Solución alternativa

Utilice la función de búsqueda en el visor de PDF para localizar manualmente la sección referenciada.

Estado

El problema está bajo investigación.

© Copyright 2026 Open Text

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