OpenText™ Core Application Security

Notas de la versión

Version : 26.2

PDF Generated on : April 22, 2026

Table of Contents

1. Notas de la versión 1

1.1. Cambios de nombre de producto de Fortify 2

1.2. Actualizaciones del motor y del paquete de reglas 3

1.3. Nuevas características 4

1.4. Problemas conocidos 11

1. Notas de la versión

Este documento proporciona las nuevas características, notas de instalación y actualización, problemas conocidos y soluciones alternativas que se aplican a la versión 26.2.0 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 26.2.0 incluye las siguientes versiones del motor y del paquete de reglas:

- **Fortify Software Security Content 26.1.0:**
  OpenText Core Application Security implementa Fortify Software Security Content 26.1. Para obtener más información, consulte Fortify Software Security Content 26.1.
- **OpenText Static Application Security Test 26.1.0:**
  OpenText Core Application Security implementa OpenText SAST (Fortify Static Code Analyzer) versión 26.1.

1.3. Nuevas características

SAST impulsado por IA

La función Core Application Security ahora incluye soporte para análisis con inteligencia artificial para 12 lenguajes de programación adicionales, gracias a nuestra arquitectura SAST de próxima generación. Esta arquitectura mejorada acelera significativamente la incorporación de nuevos idiomas, lo que permite ofrecer soporte para futuros idiomas de forma más rápida y eficiente. Para habilitar esta función, se encuentra disponible una nueva configuración, Habilitar SAST impulsado por IA, en Administración → Configuración → SAST.

Para obtener más información, consulte Configuración de SAST en la Guía del usuario de Core Application Security.

Note

Esta función se ha lanzado, pero actualmente no está disponible. Se habilitará en una fecha posterior.

Mejoras en el panel de control de corrección

Core Application Security 26.2 introduce los siguientes gráficos en el nuevo panel de control de corrección:

- Revisar la cobertura por gravedad: muestra el porcentaje de problemas de seguridad identificados que se han revisado en cada nivel de gravedad.
- Cobertura de corrección por gravedad: muestra el porcentaje de problemas corregidos por nivel de gravedad, lo que pone de manifiesto la eficacia con la que se abordan las vulnerabilidades de mayor riesgo.
- Tendencia de corrección de problemas: muestra las tendencias mensuales de corrección de problemas según su gravedad para facilitar la planificación, la priorización y la asignación de recursos.
- Problemas que se reabren con frecuencia: muestra una lista clasificada de las categorías de problemas de seguridad que se reabren con mayor frecuencia, lo que ayuda a identificar áreas que requieren un análisis más profundo de la causa raíz o mejoras en los procesos.
- Revisar la cobertura por tipo de análisis: muestra el porcentaje de problemas corregidos según el tipo de análisis, lo que indica la eficacia de la corrección en diferentes enfoques de pruebas de seguridad.

- Cobertura de corrección por tipo de análisis: muestra el porcentaje de problemas corregidos según el tipo de análisis.
- Adopción de SAST Aviator: muestra un resumen visual de la adopción de SAST Aviator en todas las aplicaciones gestionadas.
- Tiempo medio de corrección: esta vista resalta la mejora en los plazos de corrección en comparación con el año anterior y muestra claramente el cambio interanual (YoY).
- Tiempo medio de corrección por gravedad: muestra el tiempo medio de corrección desglosado por nivel de gravedad, lo que demuestra la eficacia con la que se priorizan los problemas de mayor riesgo.
- Tasa de reapertura de problemas muestra el porcentaje actual de problemas reabiertos, incluyendo el número exacto de casos.
- Retorno de la inversión (ROI) de SAST Aviator: muestra los ahorros financieros estimados y la eficiencia en el tiempo logrados a través de SAST Aviator, destacando el valor comercial de la detección y corrección temprana de vulnerabilidades.

Para obtener más información, consulte Paneles nuevos en la Guía del usuario de Core Application Security.

Escaneo DAST protegido con autenticación de dos factores

La función Core Application Security ahora admite el análisis dinámico de aplicaciones protegidas por la autenticación de dos factores (2FA). Esta mejora permite evaluar de forma segura las aplicaciones que requieren autenticación multifactor, manteniendo al mismo tiempo sólidos controles de acceso. Para respaldar esta funcionalidad, el formulario de configuración de DAST se ha actualizado con campos de configuración adicionales, lo que permite a los equipos proporcionar los detalles de autenticación necesarios para las aplicaciones habilitadas para autenticación de dos factores y ejecutar análisis dinámicos correctamente.

Para obtener más información, consulte Configuración de análisis dinámicos en la Guía del usuario de Core Application Security.

Soporte para la integración de SCIM

Core Application Security 26.2 introduce una nueva función de integración SCIM que permite el aprovisionamiento automatizado de usuarios y grupos entre el proveedor de identidades (IdP) del cliente y su inquilino, en consonancia con el estándar SCIM

2.0. Para respaldar esta capacidad, se necesita una nueva pestaña de Integración SCIM en Administración → Administración de usuarios en el portal del inquilino. Esta interfaz especial proporciona la configuración y la administración centralizadas del aprovisionamiento basado en SCIM.

Para obtener más información, consulte Configuración del sistema para la gestión de identidades entre dominios (SCIM) en la Guía del usuario de Core Application Security.

Integración de SCIM con registro único (SSO)

Además, ahora se puede habilitar el aprovisionamiento SCIM directamente a través del registro único (SSO). Al habilitar SCIM desde la configuración de SSO, las organizaciones pueden optimizar la autenticación de identidades y la gestión del ciclo de vida dentro de un flujo de trabajo único y centralizado.

Para obtener más información, consulte Configuración de SSO en OpenText Core Application Security en la Guía del usuario de Core Application Security.

DAST: disponibilidad del árbol del sitio para análisis manuales

La función Core Application Security ahora proporciona acceso a los árboles del sitio capturados durante los análisis manuales dinámicos de aplicaciones web. Esta capacidad permite una mayor visibilidad de la estructura de las aplicaciones escaneadas y facilita un análisis y una revisión más eficaces. El archivo de los árboles del sitio está disponible para su descarga directamente desde la página de análisis.

Para obtener más información, consulte Visualización de análisis de versión en la Guía del usuario de Core Application Security.

Resultados DAST manuales y automatizados agrupados

Core Application Security ahora permite a los clientes categorizar los resultados de Dynamic+ según si se descubrieron mediante evaluaciones manuales o análisis automatizados, lo que ofrece una mayor claridad sobre cómo se detectan las vulnerabilidades.
Para obtener más información, consulte Visualización de análisis de versión en la Guía del usuario de Core Application Security.

Actualizaciones de los estándares de seguridad

Core Application Security ahora ofrece compatibilidad total con los últimos estándares de seguridad del sector, lo que mejora la generación de informes, el análisis y la administración de directivas en toda la plataforma.
Las siguientes funciones ahora son completamente compatibles:

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

Función de clave de API para la administración de usuarios

Core Application Security 26.2 introduce una nueva función de clave de API, Administrar usuarios, que permite la administración de usuarios y grupos de usuarios mediante API sin necesidad de permisos elevados. Esta nueva función le permite automatizar e integrar los flujos de trabajo de administración de usuarios de forma más segura y eficiente, manteniendo al mismo tiempo los controles de acceso adecuados.

Para obtener más información, consulte Roles de la clave de API en la guía del usuario de Core Application Security.

Cambios en las notificaciones del sistema

A partir de Core Application Security 26.2, los líderes en seguridad reciben automáticamente notificaciones de correo electrónico cada vez que se modifican los ajustes de registro único (SSO) del inquilino. Esta mejora aumenta la visibilidad de los cambios de configuración relacionados con la identidad y ayuda a garantizar el conocimiento y la gobernanza oportunos de los ajustes de autenticación.

Aprovisionamiento de derechos de desarrollador

La función Core Application Security ahora incluye mejoras en la página de derechos para admitir licencias basadas en desarrolladores. Los administradores de inquilinos pueden configurar los derechos de acceso basados en desarrolladores durante la configuración del inquilino y administrarlos junto con las licencias basadas en aplicaciones. Ahora, todos los tipos de derechos se muestran en una única interfaz consolidada, lo que facilita la visualización de los totales, el seguimiento del consumo, la supervisión de la disponibilidad y la revisión de los detalles de vencimiento. Estas mejoras simplifican la gestión de derechos y proporcionan una

mayor transparencia en todos los modelos de licenciamiento.

Para obtener más información, consulte Visualización de derechos en la Guía del usuario de Core Application Security.

Compatibilidad ampliada con las versiones de CycloneDX

Core Application Security ahora amplía su capacidad de importación de CycloneDX SBOM para incluir archivos JSON que cumplen con la especificación CycloneDX 1.7. Las versiones compatibles anteriormente permanecen sin cambios, y esta actualización amplía la compatibilidad al último estándar CycloneDX.

Para obtener más información, consulte Importando de en la lista de materiales de software en la Guía del usuario de Core Application Security.

Configuración de atributos mejorada

Ahora puede habilitar simultáneamente las opciones "Obligatorio" y "Solo los líderes en seguridad pueden editarlo" al configurar los atributos. Cuando se seleccionan ambas opciones, el sistema ahora requiere un valor predeterminado para garantizar que el atributo se complete correctamente durante la creación de la entidad. Para los atributos de "Lista de selección", este valor predeterminado debe seleccionarse de entre los valores de la lista disponibles.

Para obtener más información, consulte Adición de un atributo en la guía del usuario de Core Application Security.

Compatibilidad de MAST+ con campos de credenciales adicionales

La configuración de MAST+ ahora admite flujos de trabajo de autenticación más avanzados. Puede agregar hasta tres campos de credenciales adicionales para la autenticación de formularios durante los análisis MAST+.

Para obtener más información, consulte Configuración de análisis móviles 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:

- El extremo de edición masiva de vulnerabilidades se ha mejorado para admitir escenarios de actualización más amplios:
  - `POST /api/v3/releases/{releaseId}/vulnerabilities/bulk-edit`

  Este extremo ahora incluye un parámetro booleano opcional, includeAllVulnerabilities, que permite aplicar actualizaciones masivas a todas las vulnerabilidades asociadas con una versión, sin necesidad de Id. individuales de vulnerabilidad o problema. Esto simplifica las actualizaciones de corrección a gran escala y los flujos de trabajo de automatización.

- Los siguientes extremos de atributos ahora admiten configuraciones en las que se pueden habilitar simultáneamente tanto Necesario como Restringido (Solo los líderes en seguridad pueden editarlo):
  - `POST /api/v3/attributes`
  - `PUT /api/v3/attributes/{attributeId}`

  Esta mejora garantiza la paridad con la configuración de atributos basada en la interfaz de usuario y aplica una gobernanza de datos coherente durante la creación de entidades.

- Los siguientes extremos de análisis estático se han mejorado para admitir SAST impulsado por IA:
  - `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`

  Estas actualizaciones permiten a los clientes integrar sin problemas el análisis estático basado en IA en sus flujos de trabajo automatizados.

- Se han añadido nuevos puntos de acceso para la generación de informes con el fin de admitir la exportación y el procesamiento automatizados de datos, eliminando la necesidad de realizar acciones manuales en el portal:
  - GET /api/v3/reports/dataexports/templates - Recupera las plantillas de exportación de datos disponibles.
  - POST /api/v3/reports/dataexports - Inicia una nueva exportación de datos.
  - GET /api/v3/reports/dataexports/{dataExportId} - Recupera el estado y los detalles de una exportación de datos específica.

- Como parte de las capacidades de licencia basadas en desarrolladores, los siguientes extremos ahora admiten la captura de la información de licencia basada en desarrolladores:
  - `GET /api/v3/tenant-entitlements`
  - `GET /api/v3/tenant-open-source-entitlements`

1.4. 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.

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