OpenText™ Core Application Security

Notas de la versión (25.3.0)

Version : 25.3

PDF Generated on : September 10, 2025

Table of Contents

1. Notas de la versión (25.3.0)

Este documento proporciona las nuevas características, notas de instalación y actualización, problemas conocidos y soluciones alternativas que se aplican a la versión 25.3.0 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. Anuncios

En la versión 25.3.0 de Core Application Security:

- La versión 25.2.0 de SAST Aviator ya está disponible para los usuarios.
- La versión 25.2.0 de ScanCentral ya está disponible para los usuarios.
- La versión 25.2.0 de pruebas de seguridad de las aplicaciones dinámicas de OpenText™ (OpenText DAST) ya está disponible para los usuarios.
- El soporte para la versión 5.3 de STIG está obsoleto.
- La compatibilidad con PCI 2.0 DSS Compliance y PCI 3.0 DSS Compliance también está obsoleta.

1.3. Nuevas características

Nueva evaluación manual de DAST

A partir de la versión 25.3.0, se ofrece la posibilidad de evaluación manual dinámica para ayudar a los clientes con aplicaciones web que son difíciles o complicadas de analizar utilizando escáneres automáticos. *Para obtener más información, consulte "Configuración de análisis dinámicos" en la Guía del usuario de Core Application Security.*

Inicio de sesión en el portal 2FA basado en TOTP

A partir de la versión 25.3.0, Core Application Security admite TOTP como una opción adicional para la autenticación en dos fases (2FA). *Para obtener más información, consulte "Configuración de seguridad de usuarios" en la Guía del usuario de Core Application Security.*

Actualizaciones de SSO

Compatibilidad con aserciones SAML cifradas

Core Application Security ahora le permite solicitar un nuevo certificado de cifrado SAML y usarlo para el cifrado de afirmaciones en el lado del proveedor de identidad. *Para obtener más información, consulte "Configuración de cifrado" en la Guía del usuario de Core Application Security.*

Excluir usuarios o dominios específicos del uso de SSO

Core Application Security ahora permite excluir dominios específicos de la configuración de SSO. Si hay usuarios en el inquilino de diferentes dominios, puede especificar la lista de dominios o usuarios que se excluirán del requisito de inicio de sesión SSO. *Para obtener más información, consulte "Configuración de SSO en OpenText Core Application Security" en la Guía del usuario de Core Application Security.*

Otras actualizaciones del portal

Compatibilidad con DISA STIG 6.2, PCI DSS 4.0.1 y 2024 CWE Top 25

Core Application Security ahora es compatible con DISA STIG 6.2, PCI DSS 4.0.1 y el estándar 2024 CWE Top 25. El portal se ha actualizado con las siguientes soluciones:

- Se han agregado nuevos módulos de informes y plantillas para DISA STIG 6.2, PCI DSS 4.0.1 y 2024 CWE Top 25.
- La exportación de datos de problemas ahora incluye columnas para DISA STIG 6.2, PCI DSS 4.0.1 y 2024 CWE Top 25.
- DISA STIG 6.2, PCI DSS 4.0.1 y 2024 CWE Top 25 se han incorporado a las listas de agrupación y filtros en las páginas Problemas de aplicación y Problemas de versión.
- Al crear una política de seguridad, DISA STIG 6.2, PCI DSS 4.0.1 y 2024 CWE Top 25 ahora están disponibles en la lista de clasificaciones.
- Los puntos finales de API que brindan detalles de vulnerabilidad se han actualizado para incluir detalles de PCI DSS 4.0.1 y 2024 CWE Top 25.

Opción para deseleccionar problemas individuales de la selección de grupo en la página Problemas

A partir de la versión 25.3.0, en la página Problemas, los clientes pueden deseleccionar los problemas individuales. *Para obtener más información, consulte "Visualización de los problemas de versión" en la Guía del usuario de Core Application Security.*

Página de análisis: señal visual que indica cambios en la carga útil desde el último análisis SAST

A partir de la versión 25.3.0, en la página Análisis, los clientes pueden ver la diferencia en las cargas útiles entre los análisis actuales y los anteriores. *Para obtener más información, consulte "Visualización de todos los análisis" en la Guía del usuario de Core Application Security.*

Página de resumen de análisis: disponibilidad de tiempos de cola de SAST

A partir de la versión 25.3.0, los clientes pueden ver el tiempo de cola de análisis en la página Resumen de análisis. *Para obtener más información, consulte "Visualización de todos los análisis" en la Guía del usuario de Core Application Security.*

Actualización del formulario de configuración dinámica

A partir de la versión 25.3.0, Core Application Security admite 3 campos de credenciales adicionales para la autenticación de formularios durante la evaluación manual dinámica+ y DAST. *Para obtener más información, consulte "Configuración de análisis dinámicos" en la Guía del usuario de Core Application Security.*

Restricciones de IP restablecidas

A partir de la versión 25.3.0, la función de restricciones de IP se ha restaurado por completo. *Para obtener más información, consulte "Configuración de seguridad de usuarios" en la Guía del usuario de Core Application Security.*

Renombrado de Fortify Aviator a SAST Aviator

A partir de la versión 25.3.0, la versión Aviator 25.2 se denomina SAST Aviator. Igualmente se actualiza en el portal y en la documentación del producto.

Enlace de Marketplace al código de corrección de Visual Studio Code

El enlace al código de código de corrección de Visual Studio Code ahora está disponible en la página de herramientas.

Actualizaciones de la API

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

- Se agrega el nuevo parámetro de solicitud includeSystemEvents al extremo de API GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/history para incluir eventos del sistema en el punto final del historial.

  El valor predeterminado es **false**. Si el valor se establece en **false**, entonces no hay eventos del sistema incluidos en la respuesta. Si el valor se establece en **true**, los eventos del sistema se capturan en los datos de respuesta.

- La funcionalidad de los siguientes puntos finales está alineada garantizando la paridad de características entre ellos:
  - POST/api/v3/releases/{releaseid}/static-scansand start-scan-advanced
  - POST/api/v3/releases/{releaseid}/static-scansand start-scan
- Los siguientes extremos de API se modifican para utilizar el valor VulnId o Id en lugar del parámetro VulnId:
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId} (devuelve una lista de vulnerabilidades)
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/all-data (devuelve todos los datos de la vulnerabilidad)

- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/summary (devuelve el resumen de la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/details (devuelve los detalles de la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/recommendations (devuelve las recomendaciones de la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/history (devuelve el historial de la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/screenshots (devuelve las capturas de pantalla de la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/screenshot/{screenshotId} (devuelve una captura de pantalla)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/request-response (devuelve la solicitud y la respuesta de la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/headers (devuelve los encabezados de la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/parameters (devuelve los parámetros de la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/traces (devuelve los seguimientos de la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/traces/{traceIndex}/{traceEntryIndex}/code (devuelve el código de seguimiento de un índice concreto)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/traces/{traceIndex}/{traceEntryIndex}/snippet (devuelve el fragmento de seguimiento fragmento índice concreto)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/audit-options (devuelve las opciones de auditar la vulnerabilidad)
- GET /api/v3/releases/{releaseId}/vulnerability-filters (abre los filtros de vulnerabilidad disponibles)
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/comments (devuelve los comentarios de auditar la vulnerabilidad)

1.4. Funciones no compatibles con esta versión

Las siguientes funciones ya no son compatibles.

- Las versiones del informe de cumplimiento anteriores a 2014 quedan obsoletas a partir de:
  - Plantilla de informe y módulos
  - Funcionalidad para la exportación de datos
  - Opciones de agrupación y filtrado en la página Problemas del inquilino
  - Administrador de directivas
  - API
- Todas las funcionalidades relacionadas con STIG 5.1 y 5.2 quedan obsoletas.

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