OpenText™ Fortify Code Security Extension for Visual Studio Code

Release notes

Version 26.4

PDF Generated on September 10, 2026

Table of Contents

Release notes

Software Version: 26.4

Software Release Date: September 11, 2026

Document Release Date: September 11, 2026

This release includes changes from the previous patch and introduces enhancements across several key areas of the product.

What's new in Fortify Code Security Extension for Visual Studio Code

Automatic skill updates through FCLI

Fortify skills and agents are now dynamically updated through FCLI. This enhanced functionality automatically retrieves new skills and updates when you install or start VS Code and makes them available directly in the IDE.

Fortify MCP servers in VS Code

VS Code now includes support for the following Fortify MCP servers:

- OpenText™ Core Application Security
- OpenText™ Application Security
- OpenText™ ScanCentral SAST
- OpenText ScanCentral DAST
- Aviator

Automatic remediation through Core Application Security

You can now automatically apply Fortify Aviator remediation fixes directly from the IDE for issues identified through scans performed in Core Application Security. The IDE highlights issues with available fixes and lets you view remediation details and apply fixes.

Support for Amazon Web Services Kiro and Google Antigravity

The VS Code extension now supports Kiro and Antigravity. You can access the same UI and AI capabilities available in VS Code in these VS Code-based IDEs. You can download and install these IDEs from AWS Marketplace and Google Cloud Marketplace.

Auto remediation support for all Application Security remediation modes

Enhanced auto remediation to support remediation based on selected Fortify Project Report (FPR) scan results. You can choose whether to generate remediations from all scans, the latest scan, or scans within a selected date range.

AI assistant chat support for skills and Model Context Protocol selection

You can now choose whether your Fortify AI assistance experience is powered by skills or Model Context Protocol (MCP). The selected option, **Skills (Chat Skills)** or **MCP (MCP Server Tools)** determines how the AI assistant uses Fortify capabilities in VS Code.

Build tool integration for local SAST scans

Local SAST scan configuration now supports build tool integration. You can include build commands and options for tools such as Maven, Gradle, MSBuild and other supported build systems.

Fixed issues

The patch includes bug fixes and quality enhancements that improve application stability in Fortify Code Security Extension for Visual Studio Code:

- Fixed an issue where creating an application in Application Security Center failed when mandatory custom attributes of type Integer or Date were configured in Application Security Center.

  Note
  You must update the fcli to version 3.20.0.

Known issues

- When a OpenText Core Application Security and Application Security Center session is created through the Command Palette by running the `fcli` command, the **Refresh** button in the extension does not update the displayed login status.
- Saved OpenText Core Application Security and Application Security Center session credentials persist even after the Fortify Code Security extension is uninstalled and reinstalled.
- After setting a preferred platform (OpenText Core Application Security or Application Security Center) in the extension settings, the **Quick Links** section does not correctly filter the quick links based on the selected platform.
- When executing certain fcli commands using the **Execute via Dialog** option, the extension displays the fcli help page in the **Output** console if the dialog contains required fields.
- When users click options in the Fortify Code Security sidebar before completing required prerequisite steps, the extension does not display an appropriate validation or guidance message.
- When executing a fcli command using the **Execute via Dialog** option, the entered data is cleared once the command completes and results are displayed.
- When using the `FCli SSC create-template` or `FCli FoD create-template` command via the Command Palette, the **Template Path** field is not auto-populated and does not provide suggestions or a file selection option.
- When remediating and auditing Core Application Security vulnerabilities, selecting an **Assigned User** is mandatory. Otherwise, the audit fails.
- In Core Application Security remediation workflow, the **Pending Review** status is not available in the **Auditor Status** list. The **Auditor Status** list reflects values from the Core Application Security portal level instead of being scoped to the release level.

Support

If you have questions or comments about using this product, contact Customer Support. When contacting Customer Support, provide the following product information:

Software Version: 26.2.2

Software Release Date: June 12, 2026

To manage your support cases, acquire licenses, and manage your account: https://portal.microfocus.com/

Legal Notices

Warranty

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