OpenText™ Fortify Code Security Extension for Visual Studio Code

Release Notes

Version : 26.2

Table of Contents

1. Release Notes

Fortify Code Security Extension for Visual Studio Code Release Notes

Software Version: 26.2

Software Release Date: April 2026

Document Release Date: April 2026

Fortify Code Security Extension for Visual Studio Code

The Fortify Code Security Extension for Visual Studio Code provides an integrated application security workflow inside Visual Studio Code to support early identification and remediation of vulnerabilities. Use the Fortify Code Security Extension for Visual Studio Code to authenticate, select target applications, run scans, and remediate findings across OpenText Core Application Security and Application Security Center.

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.
- During initial configuration of the extension, the **Browse** button for selecting the `fcli` executable and Fortify Static Code Analyzer executable in the workspace settings does not respond.

  Workaround:

  - Manually enter the full file path for `fcli` and `sourceanalyzer` executable into the corresponding workspace settings fields.
  - Restart VS Code after saving the settings or use the `Developer: Reload Window` command to reload VS Code.
- When you click **SETTINGS** in the sidebar, the **Settings** box displays `No Settings Found`.

  Workaround: In the **Search Settings** box, change the `@ext:OpenText.fortify-code-security` search text to `@ext:fortifyvsts.fortify-code-security`.
- 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.
- When remediating and auditing Application Security Center issues, the value for custom tag of the `date` type is not retrieved from Application Security Center and are not displayed in the **Audit** panel.
- When remediating and auditing Core Application Security vulnerabilities, analysis trace icons are not displayed.

- 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.

- When the **ScanCentral Client: Auto Update** setting is enabled, the latest ScanCentral client is installed successfully. However, after restarting the extension, the **ScanCentral Client: Executable Path** in the extension settings is not updated automatically, and the **ScanCentral Client: Auto Update** setting is disabled (unchecked) automatically.

  Workaround:
  After restarting the extension:

  - Manually update the **ScanCentral Client: Executable Path** to point to the newly installed client.
  - Re-enable Auto Update if required.

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: 26.2.0

Software Release Date: April 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