OpenText™ Fortify Code Security Extension for Visual Studio Code

Patch Release Notes

Version : 26.2.1

© Copyright 2026 Open Text

1. Patch Release Notes

Fortify Code Security Extension for Visual Studio Code Patch Release Notes

Software Version: 26.2.1

Software Release Date: June 5, 2026

Document Release Date: June 5, 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.

New features

This patch includes the following features for Fortify Code Security Extension for Visual Studio Code:

- Debug level logs.
- Latest `@fortify` skills.
- Secure Code Warrior links in the **Recommendations** tab in the **REMEDIATE** section for OpenText Core Application Security workflows.
- Standards and best practices information from Fortify Software Security Research in the **Vulnerabilties** tab in the **REMEDIATE** section for OpenText Core Application Security workflows.
- Search functionality to search for release names or version names in the **Select Application** area, **CREATE / MODIFY APPLICATION & VERSION** panel, and **CREATE/MODIFY APPLICATION & RELEASE** panel for OpenText Core Application Security and Application Security Center workflows.
- Search functionality to search for an user to assign to the issue from **Assigned User** list or **User** list in **AUDIT** panel on the **REMEDIATE** section for OpenText Core Application Security or Application Security Center workflows.
- Search for all the application names in the **Select Application** area, **CREATE / MODIFY APPLICATION & VERSION** panel, and **CREATE/MODIFY APPLICATION & RELEASE** panel for OpenText Core Application Security and Application Security Center workflows. Previously, when you searched for an application, the

extension searches only within the initial 50 entries and to search additional entries, you need the next set of 50 entries.

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 while remediating and auditing Core Application Security vulnerabilities, analysis trace icons were not displayed.
- Fixed an issue where during initial configuration of the extension, the **Browse** button for selecting the `fcli` executable and Fortify Static Code Analyzer executable in the workspace settings did not respond.
- Fixed an issue where creating an application or release in **Core Application Security** automatically assigned the first available user as the owner instead of requiring users to explicitly select an owner.
- Fixed an issue where updating or creating a release in **Core Application Security** also triggered an unnecessary application update, even when no changes were made to application attributes.
- Fixed an issue where scan actions continued to use a previously selected release ID in **Core Application Security** after creating a new application or release, causing View/Edit settings and scan operations to run against an outdated release.
- Fixed an issue where the **Scan Settings** options **View/Edit** and **Upload File** options were enabled simultaneously instead of being mutually exclusive based on the selected scan configuration.
- Fixed an issue where the **Settings** view displayed `No Settings Found` when accessed from the sidebar due to an incorrect search text being applied in the **Search Settings** box.
- Fixed an issue where value for custom tag of the `date` type were not retrieved from **Application Security Center** and were not displayed in the **Audit** panel during remediation and audit workflows.
- Fixed an issue where application and version selections from a previous session were not validated after switching to a different **Application Security Center** or **Core Application Security** instance, causing outdated values to persist.
- Fixed an issue and improved performance where the **Audit** panel in **Core Application Security** triggered repeated API calls when switching between Analysis Trace, Vulnerability, Recommendations, and History, causing unnecessary delays while navigating the UI.
- Fixed multiple UI issues in the **Audit** panel in **Core Application Security**, including inconsistent loading indicators, inability to deselect selected issues, premature

stopping of loading indicators during remediation, refresh not updating history data, and unintended issue selection when clicking outside checkboxes.
- Fixed an intermittent issue where the **Audit** panel became unresponsive when saving comments in Core Application Security workflows.
  Fixed an issue where the **Auto Remediate** button was enabled even when no active session was available, allowing users to initiate remediation without authentication.
- Fixed an issue where enabling **ScanCentral Client: Auto Update** did not persist the executable path after restarting the extension and automatically disabled the Auto Update setting.
- Fixed an issue where entering an invalid fcli executable path caused duplicate validation errors to be displayed in the **Settings** view.

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.

- Creating an application in Application Security Center fails when mandatory custom attributes of type Integer or Date are configured in Application Security Center.

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: 26.2.1

Software Release Date: June 5, 2026

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

Legal Notices

Copyright 2026 Open Text

Warranty

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

© Copyright 2026 Open Text

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