

CVE-2026-89332 - Kiro IDE Sensitive Workspace Data Exfiltration via Agent-Written Workspace Configuration

Bulletin ID: 2026-111-AWS
Scope: AWS
Content Type: Important (requires attention)
Publication Date: 09/11/2026 12:00 PM PDT

Description:

Kiro IDE is an agentic development environment that makes it easy for developers to ship real engineering work with the help of AI agents.

We identified [CVE-2026-89332](#), where the Kiro agent could modify a workspace's settings file in an untrusted workspace in Kiro IDE. A specially crafted repository could use this to point the Kiro Powers registry URL, which Kiro fetches when the Powers panel is opened, at an external endpoint, sending potentially sensitive workspace data to that endpoint. Kiro presented the edit to the user for approval, showing the inserted data and the URL, but the file was already written to disk, so opening the Powers panel before responding to the prompt made the request anyway.

Impacted versions: Kiro IDE < 0.8.135

Resolution:

This issue has been addressed in [Kiro IDE version 0.8.135](#) and greater. We recommend upgrading to the latest version and rotate any credentials present in a project opened on an earlier version.

Workarounds:

None.

References:

- [CVE-2026-89332](#)

Please email aws-security@amazon.com with any security questions or concerns.



Learn	+
Resources	+
Developers	+
Help	+

Amazon is an equal opportunity employer and does not discriminate on the basis of protected veteran status, disability or other legally protected status. Veterans, military spouses, and people with disabilities are encouraged to apply.

