



CVE-2026-0830 - Command Injection in Kiro GitLab Merge Request Helper

Bulletin ID: 2026-001-AWS

Scope: AWS

Content Type: Important (requires attention)

Publication Date: 2026/01/09 13:15 PM PST

Description:

Kiro is an agentic IDE users install on their desktop. We identified [CVE-2026-0830](#) where opening a maliciously crafted workspace may lead to arbitrary command injection in Kiro IDE before Kiro version 0.6.18. This may occur if the workspace has specially crafted folder names within the workspace containing injected commands.

Affected versions: Kiro IDE <0.6.18

Resolution:

This issue has been addressed in Kiro IDE version 0.6.18. We recommend upgrading to the latest version.



References:

- [CVE-2026-0830](#)

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

Learn

What Is AWS?

What Is Cloud Computing?

What Is Agentic AI?

Resources

Getting Started

Training

AWS Trust Center

Developers

Builder Center

SDKs & Tools

.NET on AWS

Python on AWS

Help

Contact Us

File a Support Ticket

AWS re:Post

Knowledge Center

- Cloud Computing
- Concepts Hub
- AWS Cloud Security
- What's New
- Blogs
- Press Releases
- AWS Solutions Library
- Architecture Center
- Product and Technical FAQs
- Analyst Reports
- AWS Partners
- Java on AWS
- PHP on AWS
- JavaScript on AWS
- AWS Support Overview
- Get Expert Help
- AWS Accessibility
- Legal



Amazon is an Equal Opportunity Employer: Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.



[Back to top](#) ↑



[Privacy](#) [Site terms](#) [Your Privacy Choices](#) [Cookie Preferences](#)

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.