CVE-2025-55190

08/09/2024

Sensitive Repository Credential Disclosure in Argo CD Across Multiple Versions

CONFIDENTIAL

Executive Summary

Argo CD is a Kubernetes-native continuous deployment (CD) and GitOps tool.

API tokens (in the versions mentioned below) with project-level permissions can retrieve sensitive repository credentials (usernames, passwords) through the project details API endpoint, even when the token only has standard application management permissions and no explicit access to secrets

Analysis

Affected Versions: 2.13.0 through 2.13.8, 2.14.0 through 2.14.15, 3.0.0 through 3.0.12 and 3.1.0-rc1 through 3.1.1,

This vulnerability does not only affect project-level permissions. Any token with project get permissions is also vulnerable, including global permissions such as: `p, role/user, projects, get, *, allow`.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/200.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-55190

Solutions

This issue is fixed in versions 2.13.9, 2.14.16, 3.0.14 and 3.1.2.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.