GUIDE

Critical Argo CD API Flaw (CVE-2025-55190) Leaks Repository Credentials

> 🚨 **CRITICAL** — Security fix. Upgrade immediately.

> **Version:** 3.1.2, 3.0.14, 2.14.16, 2.13.9 | **Released:** 2026-05-26 | **Upgrade from:** Multiple affected versions (see details)

Release at a Glance

A critical security vulnerability, **CVE-2025-55190**, has been identified and patched in Argo CD. This flaw allows project-level API tokens to expose sensitive repository credentials, posing a significant risk to CI/CD pipelines.

Here's what you need to know immediately:

- **Critical Vulnerability:** Project-level API tokens in affected Argo CD versions can retrieve repository usernames and passwords, even without explicit secret access permissions.
- **Immediate Action Required:** All users running affected Argo CD versions **must upgrade immediately** to a patched version.
- **Impact:** This vulnerability can lead to unauthorized access to your source code repositories, enabling supply chain attacks and compromising your infrastructure.
- **Fixed Versions:** Upgrade to Argo CD **3.1.2, 3.0.14, 2.14.16, or 2.13.9** to remediate this issue.

Security Fixes: CVE-2025-55190

Today, we are releasing urgent patches for Argo CD to address a critical security vulnerability, **CVE-2025-55190**, titled "Project API Token Exposes Repository Credentials." This flaw was discovered by Ashish Goyal and impacts the confidentiality of your repository access.

What is CVE-2025-55190?

This CVE describes an information disclosure vulnerability where Argo CD API tokens, specifically those with project-level permissions, could retrieve sensitive repository credentials. This includes usernames and passwords used to access your Git repositories. The critical aspect is that this exposure occurred even when these tokens lacked explicit permissions to access secrets, bypassing intended security controls.

The fix addresses the underlying issue that allowed these tokens to inadvertently access and expose credential data through specific API endpoints.

Technical Details of the Vulnerability

The core of CVE-2025-55190 lies in how Argo CD's Project API handled certain requests involving repository information. Argo CD uses project-level tokens to automate deployments and manage applications within defined projects. These tokens are designed to operate with a scoped set of permissions.

The Flaw Explained: An attacker or an internal actor with a project-level API token, even one with minimal `get` permissions, could interact with specific API endpoints. These endpoints, under certain conditions, would inadvertently return the sensitive repository credentials (such as `username` and `password`) associated with that project's configured repositories. This bypasses the standard authorization checks that should prevent tokens without explicit secret access from retrieving such information.

Essentially, the API was not sufficiently sanitizing or redacting the output when queried by a project token, leading to an unintended information leak. This means that a token intended only for deployment automation could be leveraged to extract the very credentials it uses for cloning and syncing repositories.

Impact on CI/CD Pipelines and Security

The implications of CVE-2025-55190 are severe, particularly for organizations relying on Argo CD for GitOps and continuous delivery:

- **Unauthorized Repository Access:** The most immediate threat is the compromise of your Git repository credentials. An attacker gaining access to these credentials could then clone private repositories, inject malicious code, or tamper with your application's source code.

- **Supply Chain Attacks:** With access to repository credentials, an attacker could initiate supply chain attacks by introducing vulnerabilities into your application's codebase or build processes. This could affect not only your applications but also your customers.
- **Privilege Escalation:** Exposed credentials could be used to access other systems or services that rely on the same authentication, potentially leading to broader network compromise.
- **Operational Disruption:** Malicious actors could disrupt your CI/CD pipelines by deleting repositories, altering deployment manifests, or preventing applications from syncing, leading to downtime and operational chaos.
- **Data Breach Risk:** If your repositories contain sensitive configuration, intellectual property, or even hardcoded secrets, their exposure through this vulnerability could constitute a significant data breach.

This vulnerability undermines the principle of least privilege, as tokens with limited permissions could access highly sensitive data.

Affected Versions and Immediate Mitigation Steps

This critical vulnerability affects multiple versions across different Argo CD release branches. It is imperative to identify your current version and upgrade without delay.

Affected Argo CD Versions:

- **2.13.x branch:** Versions 2.13.0 through 2.13.8
- **2.14.x branch:** Versions 2.14.0 through 2.14.15
- **3.0.x branch:** Versions 3.0.0 through 3.0.12
- **3.1.x branch:** Versions 3.1.0-rc1 through 3.1.1

Patched Argo CD Versions:

To remediate CVE-2025-55190, you must upgrade to one of the following versions:

- **3.1.2**
- **3.0.14**
- **2.14.16**
- **2.13.9**

Immediate Mitigation Steps:

The primary and most effective mitigation is to **upgrade your Argo CD instance immediately** to a patched version. There are no known workarounds that fully address this vulnerability without upgrading.

1. **Identify Your Current Version:** Determine which version of Argo CD you are currently running.
2. **Plan Your Upgrade:** Choose the appropriate patched version for your branch (e.g., if you are on 2.14.x, upgrade to 2.14.16).
3. **Execute Upgrade:** Follow the standard Argo CD upgrade procedures for your deployment method (Helm, Kustomize, etc.).

```
    # Example for Helm users (adjust chart version and repository as needed)
    helm upgrade argocd argo/argo-cd --version 3.1.2 -n argocd
```

```
*Replace `3.1.2` with the specific patched version relevant to your current
branch.*
```

1. **Rotate Credentials (Post-Upgrade):** As a best practice, after upgrading, consider rotating all repository credentials that were configured in Argo CD projects. This minimizes the risk if any credentials were exfiltrated before the patch was applied.
2. **Review Audit Logs:** Check your Argo CD audit logs for any suspicious activity involving project API tokens or repository access attempts, especially prior to applying the patch.

Recommended Updates for DevOps and Platform Engineers

For DevOps and Platform Engineers managing Argo CD deployments, this incident highlights several key takeaways and best practices:

- **Prioritize Security Patches:** Always stay informed about security advisories for critical infrastructure components like Argo CD. Implement a robust patch management strategy to apply security updates promptly.
- **Principle of Least Privilege:** Regularly review and enforce the principle of least privilege for all API tokens and user accounts. Ensure that tokens only have the absolute minimum permissions required for their function.

- **Credential Management:** Use secure methods for storing and managing repository credentials, such as Kubernetes Secrets, external secret management systems, or project-scoped repositories.
- **Monitoring and Alerting:** Enhance monitoring and alerting for unusual access patterns or API calls within your Argo CD environment. Look for repeated attempts to access sensitive endpoints or unexpected token usage.
- **Automated Security Scans:** Integrate automated security scanning tools into your CI/CD pipelines to detect vulnerabilities in your infrastructure and applications early.
- **Stay Updated:** Regularly consult the official Argo CD documentation and security advisories for the latest information and best practices. The official changelog for this fix can be found at Upwind Security Advisory.

This critical patch is essential for maintaining the security and integrity of your GitOps workflows. Act swiftly to protect your systems.