**Security Advisory 2023-006**

# Critical Security Flaw in Jira Service Management Server and Data Center

***February 3, 2023 — v1.0***

**TLP:CLEAR**

*History:*

- *03/02/2023 — v1.0 – Initial publication*

## Summary

A critical security flaw has been discovered in Jira Service Management Server and Data Center that can be exploited by an attacker to impersonate another user and gain unauthorized access to instances. The vulnerability is tracked as `CVE-2023-22501` with a CVSS score of 9.4 [1].

## Technical Details

If the attacker has write access to a User Directory and outgoing email enabled, it can access sign-up tokens sent to users who have never logged into their accounts. Access to the tokens can be obtained either by being included in Jira issues or requests with these users, or by gaining access to emails containing a *View Request* link. Atlassian notes that external customer accounts can be affected in projects where anyone can create their own account, even if the instance is configured with single sign-on.

## Affected Products

The vulnerability was introduced in version 5.3.0 and impacts all subsequent versions 5.3.1, 5.3.2, 5.4.0, 5.4.1, and 5.5.0. Atlassian notes that users synced to the Jira service via read-only User Directories or single sign-on (SSO) are not affected. However, external customers who interact with the instance via email are affected, even when SSO is configured. Jira sites hosted on the cloud via an `atlassian[.]net` domain are not affected.

## Recommendations

Atlassian recommends upgrading to the latest fixed versions 5.3.3, 5.5.1, and 5.6.0 or later to remediate this vulnerability. As a temporary workaround, if an upgrade is not immediately possible, a version-specific JAR file can be manually upgraded [1].

## References

[1] https://confluence.atlassian.com/jira/jira-service-management-server-and-data-center-advisory-cve-2023-22501-1188786458.html