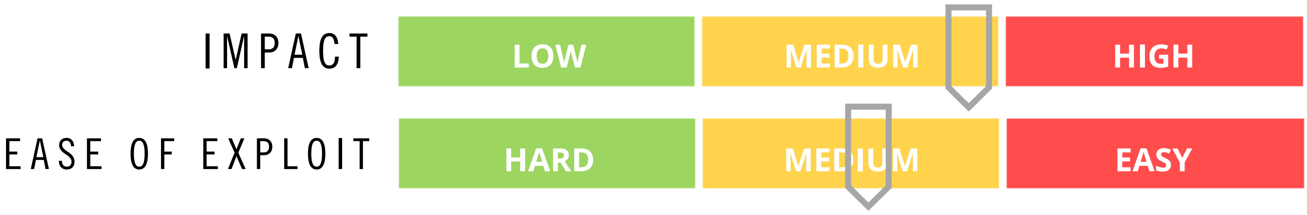
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0273

ATLASSIAN PATCHES CRITICAL FLAW IN JIRA

DATE ISSUED: 7th February 2023



OVERVIEW

Atlassian published an authentication vulnerability affecting its Jira Service Management Server and Data Center. It could allow an authenticated attacker to impersonate as a legitimate user and gain remote access to the Jira Management instance.

BREAKDOWN

If a Jira Management Service instance has a write access to a User Directory and enabled outgoing email an attacker could gain access to signup tokens sent to users with accounts that have never been logged into. Access to these tokens can be obtained in two ways:

- If the attacker is included on Jira issues or request with these users, or
- If the attacker is forwarded or gain access to emails containing a "View Request" link from these users.

Bot accounts are more susceptible to this attack due to their frequent interaction with other users and most likely to be included in Jira issues or requests. However, external customer accounts on instances with Single Sign-On (SSO) may also be affected if account creation is open to anyone. An email notification will not be generated if an attacker attempts to change the password making the attack difficult to detect. The vulnerability is tracked as CVE-2023-22501and it impacts Jira Service Management Server and Data Center version 5.3.0, 5.3.1, 5.4.0, 5.4.1, and 5.5.0. This vulnerability does not impact Jira sites which are accessed via an Atlassian.net domain.

REMEDIATION STEPS

- Upgrade to the latest versions 5.3.3, 5.4.2, 5.5.1 and 5.6.0 or later released by Atlassian.
- If the update cannot be installed immediately Atlassian has released a JAR file to update the instance manually to upgrade the "servicedesk-variable-substitution-plugin". See resource below.
- Administrators are recommended to force a password reset for all users and verify (and correct) email addresses associated with the accounts have not changed by an attacker.

REFERENCES & RESOURCES

Bleeping Computers	https://www.bleepingcomputer.com/news/security/atlassian-warns-of-critical-jira-service-management-auth-flaw/
Atlassian Support	https://confluence.atlassian.com/jira/jira-service-management-server-and-data-center-advisory-cve-2023-22501-1188786458.html