Security Advisory - May, 2022

Jira and Jira Service Management are vulnerable to an authentication bypass in its web authentication framework, Jira Seraph.

Although the vulnerability is at the core of Jira, it affects first and third-party apps like Xporter.

We recommend the upgrade of Jira as mentioned on the Atlassian Security Advisory so all apps in your instance are protected against CVE-2022-0540. As an alternative, Xporter released the 6.9.9 to the Atlassian Marketplace which fixes the vulnerability.

Xporter for Jira Server and Data Center - Authentication Bypass in Jira Seraph - CVE-2022-0540

Summary	Authentication Bypass in Jira Seraph - CVE-2022-0540
Advisory Release Date	04 May 2022 10:00 AM CET
Product	Xporter for Jira Server & Data Center
Affected on Xporter for Jira Server & Jira Data Center Versions	6.9.8 and earlier
Fixed on Xporter Jira Server & Jira Data Center Versions	6.9.9 and later

Summary of Vulnerability

This advisory discloses a security vulnerability classified as **critical** that was present in Xporter for Jira Server & Data Center. Versions of Xporter for Jira Server & Data Center affected by this vulnerability:

- 6.9.8 and earlier (fixed in 6.9.9 and later).

Customers who have upgraded Jira to a fixed version mentioned on the Atlassian Security Advisory or upgraded Xporter for Jira Server & Data Center to version 6.9.9 or higher are not affected.

Customers who are on any of the affected versions, upgrade your Jira or Xporter for Jira Server & Data Center installations immediately to fix this vulnerability.

Severity

The vulnerability is rated as critical, according to the CVSS Version 3.

Description

Jira and Jira Service Management are vulnerable to an authentication bypass in its web authentication framework, Jira Seraph.

Although the vulnerability is in the core of Jira, it affects first and third-party apps that specify `roles-required` at the `webwork1` action namespace level and do not specify it at an `action` level. For a specific action to be affected, the action will also need to not perform any other authentication or authorization checks.

A remote, unauthenticated attacker could exploit this by sending a specially crafted HTTP request to bypass authentication and authorization requirements in WebWork actions using an affected configuration.

The issue can be tracked here:

~~XPORTER-3975~~ - Authentication Bypass in Jira Seraph - CVE-2022-0540 CLOSED

Fix

We recommend the upgrade of Jira as mentioned on the Atlassian Security Advisory so all apps in your instance are protected against CVE-2022-0540. As an alternative, Xporter released the 6.9.9 to the Atlassian Marketplace which fixes the vulnerability. You can upgrade to the latest version of Xporter for Jira Server & Data Center using the Universal Plugin Manager as explained in Updating apps.

Support

If you have questions or concerns regarding this advisory, please raise a support request here.