Vulnerabilities/Threats | 3 MIN READ NEWS

Atlassian Vulnerabilities Highlight Criticality of Cloud Services

Two flaws in the popular developer cloud platform show how weaknesses in authorization functions and SaaS flaws can put cloud apps at risk.

Robert Lemos
Contributing Writer, Dark Reading

October 24, 2022

Source: Blackboard via Alamy Stock Photo

Two vulnerabilities in Atlassian Jira Align, an agile planning software-as-a-service (SaaS) tool, could allow users with access to the service to become application administrators, and then attack the Atlassian service.

That's according to cybersecurity services firm Bishop Fox, which said in an advisory today that the vulnerabilities typify the risks posed to cloud services by relatively well-known, but often hard to catch, flaws.

The two vulnerabilities found by Bishop Fox affect the Jira Align application, which is used to set agile-development goals, track efforts toward those goals, and create agile strategies. Because every instance of Jira Align is provisioned by Atlassian, an attacker could gain control of a part of the company's cloud infrastructure, Bishop Fox stated.

One vulnerability, a server-side request forgery (SSRF), could allow a user to retrieve "the AWS credentials of the Atlassian service account that provisioned the Jira Align instance," according to Bishop Fox.

The second vulnerability — in the authorization mechanism for users with the People role — could allow those users to elevate their role to Super Admin, which has access to all settings for the Jira Align tenant, such as resetting accounts and modifying settings.

The combination of the two flaws could allow a significant attack, says Jake Shafer, a security consultant with Bishop Fox, who found the flaws.

"Using the authorization finding would allow a low-privileged user to elevate their role to super admin which, in terms of information disclosure, would allow the attacker to gain access to everything the client of the SaaS had in their Jira deployment," he says. "From

However, companies should note that the increasing reliance on cloud applications has made attacks on cloud services and workloads much more common, so much so that the top class of vulnerability, according to the Open Web Application Security Project (OWASP), is broken authentication and access-control issues.

Furthermore, authorization issues are difficult for automated tools to pinpoint; plus, SSRF is a relatively new class of vulnerability that uses a cloud service's functionality and servers to conduct attacks, often bypassing security at the network edge as well as some internal security measures.

Atlassian's Jira software has already had to deal with other instances of server-side request forgery, but the company is not alone. In 2019, a former Amazon Web Services used a SSRF vulnerability to steal data from financial firm Capital One.

How to Combat Cloud Security Bugs

With cloud services becoming part of operations for the vast majority of companies, tackling the top cloud vulnerabilities is critical, Shafer says.

"With the prevalence of how integrated these SaaS applications have become in the day-to-day operations of small and large companies, it's important to remember that even these well-established companies can make mistakes," he says. "Trust but verify for all new software you'll have to be reliant on, especially something as entrenched in the tech."

These most recent vulnerabilities highlight that developers should always make sure to double-check content supplied by users before completing a request, Shafer says. Additional input-sanitization checks could prevent both attacks.

"You're allowing customers into your cloud infrastructure, they may be paying for the service but at the end of the day they should be considered just as untrusted as a potential attacker," he says.

Companies should make sure to either manually test third-party applications or reach out to the cloud provider and check the results of their security assessments. Unfortunately, automated tools are not great at discovering authorization issues, Shafer says.

"These tools rely on a set of instructions or guidelines for what to look for and dealing with authorization issues will be different for every single piece of software out there," he says. "It's very difficult to establish a set of rules that a scanner can pick up on and say 'Hey, user X shouldn't be able to do Y in the context of this specific functionality.'"

Shafer lauded Atlassian's response, saying the company "did all the right things." Atlassian did not provide a comment by publishing time.