Critical vulnerability release notes - 2022.06.30

Raley Purchase Orders got recently involved into Bugcrowd programme to make the app more secure and trustworthy for its current and prospective customers. The security testing began on 2022--05-09 and is still ongoing.

In May-June 2022 security researchers from Bugcrowd have identified several critical vulnerabilities in our app. All of the vulnerabilities listed were applicable to version 1.0.11-AC and are currently fixed in 1.0.12-AC.

1) Anonymous(JSM) user has full admin privileges

A customer user created in JSM was able to access PO configuration page meant for Jira admins only. Reported by a Bugcrowd researched and verified by our security specialist. The problem happened because of the deficiency in authorisation checks on that page from our side. To remediate this problem we've applied additional security controls to check user permissions.

Based on our access log investigations this vulnerability had no impact on our existing customers.

2) Multiple endpoints missed authorisation checks

It was found that several backend REST API's were not properly performing the authorisation checks. As such, unauthorised users were able to access /modify/delete the following entities:

- Company data
- Company approval tiers
- Department-related data
- Jira-related configuration of Raley Purchase Orders

The issue was reported by a Bugcrowd researcher and verified on our side. The problem was caused by incorrect authorisation control on the application back end, which we resolved at the same time with 1).

Based on our investigations this vulnerability was not exploited in other customers' installations.