Critical vulnerability release notes - 2021-05-06

Local file read using velocity template

Using specific Velocity statements, it was possible to read local files on Raley Emails Notifications AppServer. According to Common Vulnerability Scoring System this qualifies as critical vulnerability. The issue was identified during Bugcrowd security testing program by an independent security researcher on 2 021/05/04. The patch was implemented and rolled out to production on the same day.

Based on our investigation, such malicious Velocity statements were not used in actual configuration, thus there's very unlikely that this vulnerability have been used by a hacker.

As the app was patched immediately no further action is required from you

Anonymous user has full admin privileges

This vulnerability appeared if you have a Jira Service Management with **Can customers access and send requests from the help center without logging in** set to **Yes.**

Administration console of the Raley application could be used by an anonymous JSM user without requiring Jira ADMINISTER or SYSTEM_ADMIN privilege. According to Common Vulnerability Scoring System this qualifies as critical vulnerability

The issue was identified during Bugcrowd security testing program by an independent security researcher on 2021/05/06. The patch was implemented and rolled out to production on the same day.

As it is not possible to say whether this vulnerability have actually been exploited on real installations of Raley, we invite our users to check their existing Raley Notifications configurations for possibly suspicious configurations and if needed to remove them. If you find some notification configurations that you don't recognize, please contact us on support@raleyapps.com or raise a ticket on our helpdesk https://inversionpoint.atlassian.net/servicedesk/customer /portal/3

We'll take further actions to investigate.

We want you to know that we take those issues very seriously. We are conducting a thorough review of our internal processes to ensure this does not occur again for you and our other customers.

For any questions, please contact us via support@raleyapps.com or by raising a ticket on our JSM portal: https://inversionpoint.atlassian.net/servicedesk /customer/portal/3