RingCentral®

Tech Brief: Security QA Testing

Applicability

Security quality assurance (QA) as part of overall secure development and test cycles.

Overview

RingCentral performs rigorous testing of all products and components to ensure that they meet our standards for performance, availability, resilience, and security. This includes “security QA testing” to test the logic, security logic, and overall “fail secure” features of our products. In QA testing, security tests include explicit security test cases, such as to ensure that a user cannot authenticate with an invalid username/password. These test cases ensure that systems “fail safe”, such as disallowing access after three unsuccessful login attempts even when a login block or timeout had not been properly implemented.

Process

Secure QA testing ensures that features perform as expected and that if they do fail, they fail secure. For example, if a user logon scenario is set to temporarily lock after three failed logon attempts, fail secure would ensure that on the fourth logon attempt, nothing would happen, even if a fourth logon option was not even coded for.

While source code reviews can be performed by automated tools, RingCentral performs tool-based reviews as part of the overall build process, testing of defined test cases either manually or through automated testing, regression testing against existing functionality as part of overall regression testing and security QA testing, as well as additional manual reviews by a member of the CISO applications security team, who are independent of the overall development team.

Hands-on testing is performed on every release addressing defined test cases.

Security QA test findings are rated according to criticality; as part of our Secure Release process, no offering may be released to production if it has open Critical (P0) or High (P1) findings, including security test findings.