RingCentral

Tech Brief: Vulnerability Scanning

Applicability

Vulnerability scanning as part of the RingCentral Security Development Lifecycle.

Basis

RingCentral develops products and services with security requirements based on [OWASP](#) guidelines and [NIST](#) standards.

Process

Vulnerability scanning is the use of automated tools to analyze code for known vulnerabilities. RingCentral employs various types of vulnerability scanning during the security development lifecycle:

- **Static Application Security Testing (SAST).** Performed on the RingCentral codebase to reveal unsecure coding patterns. Also called Static Code Analysis (SCA).
- **Open-Source Software Vulnerability Scan.** Performed specifically on open-source and third-party software inclusions on the RingCentral codebase to find outdated or vulnerable libraries.
- **Open-Source Software License Verification.** Performed specifically on open-source and third-party software inclusions on the RingCentral codebase to find license issues.
- **API Vulnerability Scan.** Performed specifically on API endpoints that are deployed in the staging environment for both on premise and cloud-based endpoints, to find unsecure coding patterns.
- **Container Vulnerability Scan.** Performed specifically on image files of Docker containers to find unsecure coding patterns.
- **Mobile Application Scan.** Performed on mobile application code to find unsecure coding patterns.
- **Dynamic Application Security Testing (DAST).** Performed on the RingCentral codebase in a running state to reveal unsecure coding patterns.

For efficiency, vulnerability scanning is usually performed on code after applying secure design and threat modeling. Completing SDL as a whole provides the best assurance of developing secure products than any one of its discrete activities such as vulnerability scanning.