Tech Brief: Externally Reported Vulnerabilities & Bug Bounty Process

Applicability

Vulnerabilities in RingCentral products and services reported by external researchers.

Bug Bounty Program

RingCentral handles vulnerabilities reported through its Bug Bounty program. We use Bugcrowd to triage all externally provided reports, make sure they are within the rules of engagement, and confirm the necessary information. If the report is valid, we reward the researcher and remedy the issue.

Reporting, Triage, and Replication

The Bugcrowd bug bounty process allows external researchers to report vulnerabilities to RingCentral in a responsible and ethical manner.

Bugcrowd triages the report with a preliminary review to confirm information from the reporter, and to ensure that the report falls within the rules of engagement for externally reported vulnerabilities.

RingCentral then receives the report and attempts to replicate the reported finding. This is important as we need to ensure not only that it is real and not something that is a result of a highly misconfigured environment. By reproducing the vulnerability we are able to start the process of identifying the required remediation. If we are able to replicate the finding, then we provide a monetary reward to the researcher and remediate the issue.

Remediation

The majority of the reports we receive fall within RingCentral's purview to remediate with no action from RingCentral's customers. If a finding impacts our desktop and mobile applications, and thus may require customer actions to remediate, we will issue a Security Bulletin and an internal Customer Facing Communication to notify customers of the need to update their apps.