RingCentral

TECH BRIEF: Externally Reported Vulnerabilities & Bug Bounty Process

Applicability:

Externally reported vulnerabilities

Why:

Customers want to understand how RingCentral handles vulnerabilities reported through its Bug Bounty program.

We use Bugcrowd for our Bug Bounty program 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.

How:

RingCentral works with Bugcrowd to implement a bug bounty process for externally reported vulnerabilities. This allows external researchers to report vulnerabilities to RingCentral in a responsible and ethical manner.

What:

Bugcrowd helps by providing a review of the report, confirming information from the reporter, and ensuring that the report falls within 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, but 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.

Types of Findings:

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 applications (desktop and mobile), 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.

Published 2023