Applicability: RingCentral Products' Vulnerability Remediation

Why:

Customers often confuse product vulnerability remediation and product patching when it comes to timelines and responsibilities. Customers want to understand how RingCentral implements a product vulnerability remediation process as part of building trust in RingCentral.

What:

RingCentral's product vulnerability management discipline is tied to clearly defined timelines that drive the deadline by which an update or code change must be provided to close, or remediate, a vulnerability. These timelines ensure that highly sensitive vulnerabilities, that is, vulnerabilities that can be easily exploited, are addressed as quickly as possible. Vulnerability remediation may result in a "patch" or an update required to RingCentral's applications, or code changes within the product itself.

Once an update is available, industry-standard remediation timelines are observed, defining the timeline during which the update must be deployed. That is, the more severe the vulnerability (the more severe the consequences of it being exploited), the less time RingCentral has to deploy updates.

If the update requires customer action, such as the update of a RingCentral desktop application, then a Security Bulletin is issued. Customers are expected to complete updating their vulnerable applications within the timelines mandated by their internal patch discipline.