RESPONSIBLE SECURITY VULNERABILITY DISCLOSURE POLICY

Kinaxis appreciates the investigative work into security vulnerabilities that is carried out by well-intentioned, ethical security researchers. We are committed to working collaboratively with security researchers in resolving security issues in our product and services. This policy outlines guidelines by which Kinaxis works along with the security research community.

Please read this document carefully prior to reporting vulnerabilities[1] to ensure you understand the policy and will act in compliance with it.

If you are a security researcher and have discovered a potential or verified security vulnerability in our product or websites, we appreciate you disclosing it to us in a responsible manner and according to these guidelines. Kinaxis will analyze all vulnerability reports and implement the best course of action in a timely manner.

Reporting Guidelines

If you discover a potential or verified security vulnerability, please send an email to the Kinaxis Security, Risk & Compliance (SRC) Team at security@kinaxis.com. Refrain from using social media, as these communication channels are not actively monitored by the SRC Team for this purpose. In the email, please provide the following details:

- The exact location of the vulnerability
- A brief description of the vulnerability type (e.g. "injection")
- Full details on how to reproduce and validate the vulnerability

Important: Use our PGP key to encrypt the report before sending

VIEW PGP KEY

[1] ISO/IEC 29147:2018

You can expect the following:

- Prompt acknowledgement that your vulnerability report has been received
- Follow-up questions, if any, and a request for a call if needed
- A notification when the vulnerability is resolved

Bug Bounty

At this time, Kinaxis does not have a bug bounty program.

Disclosure Guidelines

Kinaxis appreciates the information provided by the security researchers and asks you **not** to:

- Disclose any Kinaxis' product or service vulnerabilities to third parties or the public prior to receiving confirmation from Kinaxis that the identified security issue has been resolved
- Keep or disclose any Kinaxis-owned data to any third party
- Access unnecessary amounts of data. Kinaxis estimates one to three record(s) is sufficient to demonstrate a vulnerability
- Modify data in Kinaxis systems that is not your own
- Social engineer Kinaxis staff, partners, customers or contractors
- Disrupt Kinaxis service(s) or system(s) by any means (such as DDOS, etc.)
- Breach any applicable laws and regulations

Contact

For any questions regarding this policy, please reach out to the Kinaxis Security, Risk & Compliance Team at security@kinaxis.com.