Responsible Disclosure Policy

Last Revised 11 November 2019

Overview

Saba Software is committed to keeping our products and services safe for our customers as well as their users, and data security is a top priority. If you are a security researcher and have discovered a potential security vulnerability with any Saba Software product, we encourage you to let us know right away and we appreciate your help in disclosing it to us in a responsible manner.

The Saba Security team acknowledges the valuable role that independent security researchers play in Internet security. As a result, we encourage responsible reporting of any vulnerabilities that may be found in our site or applications. Saba is committed to working with security researchers to verify and address any potential vulnerabilities that are reported to us in a responsible manner.

Please review this policy before you test and/or report a potential vulnerability. We will investigate all legitimate reports and do our best to quickly fix verified problems based on severity. This responsible disclosure program does not provide monetary rewards for bug submissions.

Testing for Security Vulnerabilities

To ensure performance, availability, and security of Saba's products and infrastructure, Saba does not allow use of Production, Trial, Sandbox, or Demo instances for security testing. Automated security scanning tools may affect the availability of our customers' data.

To conduct a security assessment of a Saba product, please contact security-disclosure@saba.com and request permission.

If you accidently find a potential security vulnerability on a production or non-production Saba instance, immediately cease testing and follow the reporting steps below.

Reporting a Potential Security Vulnerability

Privately share details of the suspected vulnerability with Saba by sending an email to security-disclosure@saba.com with "<Saba Product Name> - Potential Security Vulnerability" in the Subject line.

Provide full details of the suspected vulnerability so the Saba Security and Engineering teams may validate and reproduce the issue.

Attributes of a Good Report

Please include detailed steps in your message explaining how to reproduce the vulnerability. Include any links you clicked on, pages you visited, URLs, user IDs, etc. Images or video can be helpful. Be sure to include clear descriptions of which accounts were used and the relationships between them. If known, for each potential vulnerability, include a detailed description, impact, evidence, mitigating controls and/or remediation advice.

Conduct

While we encourage you to discover and report to us any vulnerabilities you find in a responsible manner, the following conduct is expressly prohibited:

- You do not interact with other Saba customer data, information, accounts, etc.
- You make a good faith effort to avoid privacy violations and disruptions to others, including but not limited to destruction of data and interruption or degradation of Saba's services
- You do not exploit a security issue you discover for any reason. This includes demonstrating additional risk, such as attempted compromise of sensitive company data or probing for additional issues
- You do not violate any applicable laws or regulations

We ask that you give us reasonable time to investigate and mitigate an issue you report, based on severity.

Prohibited Activities

Saba Software does not permit the following types of security research:

- Performing actions that may negatively affect Saba, its customers or its users (e.g. Spam, Brute Force, Denial of Service, etc.)
- Accessing, or attempting to access, data or information that does not belong to you
- Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to you
- Conducting any kind of physical or electronic attack on Saba personnel, property, or data centers
- Social engineering any Saba support desk, employee or contractor
- Violating any laws or breaching any agreements in order to discover vulnerabilities

Commitment

We ask that you do not share or publicize an unresolved vulnerability with others. Saba greatly appreciates the efforts of those security researchers who identify vulnerabilities and enable us to address issues that might affect our customers. We thank you for going out of your way to help us minimize the risk to our customers as well as help us in our vision to improve the overall security of our products and the Internet as a whole.