Synchronoss Vulnerability Reporting and Disclosure Process

Release Number: 2025.03

-

Table of Contents

-

Responsible Disclosure

At Synchronoss Technologies (“Synchronoss”), we prioritize the security and privacy of our applications and are committed to maintaining a safe and secure environment for our customers. We encourage security researchers who identify vulnerabilities in our products or services to report them responsibly. Synchronoss is dedicated to engaging with researchers in accordance with our Vulnerability Reporting and Disclosure Process (“Process”), ensuring that all valid security issues are assessed and addressed promptly. We remain committed to upholding the highest security and privacy standards and reserve all legal rights in cases of non-compliance.

Authorization

If you act in good faith to identify and report vulnerabilities in Synchronoss products and services while adhering to this Process, we will collaborate with you to understand and address the issues. Synchronoss will not take legal action against your vulnerability research activities, provided that you strictly comply with the guidelines outlined in this Process.

Scope

This Process applies to all products and services offered by Synchronoss. Any activities listed as prohibited below, are excluded from scope and are not authorized for testing. Moreover, vulnerabilities found in systems from vendors are also excluded from scope and should be reported directly to the vendor according to their own disclosure policy/process (if applicable).

Confidentiality

The public disclosure of any identified or alleged vulnerability, including its submission details, is strictly prohibited without the express written consent of Synchronoss. Any unauthorized disclosure will be considered non-compliance with this Process.

Guidelines

When performing your activities, you must:

- Comply with applicable laws and regulation including those related to the protection of personal data.
- Securely delete all data retrieved during your research as soon as it is no longer needed or within 30 days of the vulnerability being resolved (or as otherwise required by data protection laws).

Prohibited Actions

- **Malicious Software and Attacks**
  - Installing, transmitting, uploading, linking to, or storing malicious software.
  - Attempting or executing any form of a Denial of Service (DoS) attack.

- **Unauthorized Data Use and Distribution**
  - Installing or using devices to intercept, store, or access non-public communications.

-

- **Restricted Testing and Exploits**
    - **a.** Exploit vulnerabilities that require targeted user interaction, such as phishing and social engineering.
    - **b.** Engage in spamming activities.
    - **c.** Perform brute-force attacks targeting end users.
    - **d.** Attack systems that rely on compromised client machines.
    - **e.** Target unsupported clients.
    - **f.** Conduct tests that require physical access to servers.
    - **g.** Report purely informational vulnerabilities without security impact.
    - **h.** Test third-party applications, websites, or services that integrate with or link to Synchronoss systems.

Reporting a vulnerability

What we would like to see from you

If you believe you have discovered a security vulnerability in one of our products or services, please follow these steps to ensure we can address the issue as quickly as possible:

- **Privacy Policy:** Review our Privacy Policy before proceeding with any disclosure https://synchronoss.com/privacy-policy/
- **Responsible Disclosure:** Report your findings to us via email at *security@synchronoss.com*.
- **Description of Vulnerability:** Provide us with a detailed description about the vulnerability including:
    a. The type of vulnerability (e.g., SQL injection, cross-site scripting, etc.).
    b. The affected version(s) of our application.
    c. Impact on our customers' data or system.
    d. Determine the severity of the Vulnerability using the Common Vulnerability Scoring System. CVSS minimum acceptable version 3.1
- **Steps to Reproduce:** Provide us with sufficient information to reproduce the problem. These steps to reproduce must clearly show the impact of the described vulnerability.

How to ensure an accepted report

- **Clear and concise:** reports with well-defined contexts and accurate descriptions are highly valued and greatly increase the likelihood of acceptance.
- **Vulnerability not reproducible**: If report does not provide a clear, step-by-step guide on how to exploit the vulnerability (E.g. a proof of concept - PoC), it may not be considered exploitable and thus, rejected.
- **Vulnerability already known or previously reported**: Researching and reporting on a vulnerability that has already been reported may be considered redundant.
- **No advice offered:** Not providing viable suggestions or recommendations to mitigate the effects of vulnerabilities, such as possible workarounds or temporary fixes, may lead to rejection.
- **Relevant and focused:** reports with a streamlined presentation of facts are more likely to have a stronger impact. Adding unnecessary or extraneous details may distract from the main points and reduce the effectiveness of the report.

What you can expect from us

- In return, we promise the following when you report a vulnerability to us, that is to
    a. respond to your report promptly with our evaluation of the report.
    b. handle your report with strict confidentiality.
    c. where possible, inform you when the vulnerability has been remedied.

-