SignalWire Vulnerability Disclosure Policy

Operational policy for security researchers reporting vulnerabilities to SignalWire. Subject to legal review.

Scope

We welcome reports of security vulnerabilities affecting the systems and services listed below. Before testing, please review the in-scope and out-of-scope items carefully. If you are uncertain whether a target is in scope, do not test it, and contact us at security@signalwire.com for clarification before proceeding.

In Scope Items

The following SignalWire systems are in scope for vulnerability research:

- Production API endpoints under *.signalwire.com
- The SignalWire customer dashboard
- SignalWire-published SDKs and client libraries
- The SignalWire documentation site
- SignalWire-operated public-facing infrastructure supporting the above

Out-of-Scope Items

The following are not in scope. Reports targeting these systems will not be eligible for acknowledgment or recognition under this policy:

- **Third-party services and dependencies**, including but not limited to FreeSWITCH, which is an open-source project maintained upstream. Vulnerabilities in FreeSWITCH should be reported directly to the FreeSWITCH project.
- **Test, sandbox, staging, and pre-production environments**
- **Customer applications and integrations** built on top of SignalWire
- **Third-party services we integrate with** (e.g., carrier networks, identity providers, cloud infrastructure providers)
- **SignalWire corporate IT systems**, including employee email, internal HR systems, and corporate networks
- **Marketing websites, blog content, and non-product properties** unless they expose authenticated user data or production functionality
- **Physical security** of SignalWire offices, data centers, or staff
- **Social engineering** of SignalWire employees, contractors, customers, or partners

Out-of-Scope Findings

The following types of issues are generally not considered actionable or relevant to this policy, and we will close any reports based on these types of issues without notice:

- Denial of service or volumetric attacks
- Reports generated solely by automated scanners without manual validation or proof of exploitability
- Missing security headers without demonstrated impact
- Missing best-practice configurations (e.g., DMARC, SPF, DNSSEC) without a demonstrated exploitation path
- Self-XSS that requires the victim to paste content into their own browser
- Clickjacking on pages without sensitive state-changing actions
- CSRF on unauthenticated forms or forms with no state-changing impact
- Issues requiring physical access to a victim's device

- Issues affecting outdated browsers, operating systems, or platforms beyond their vendor support window
- Reports of publicly disclosed vulnerabilities in third-party libraries without a demonstrated exploitation path against SignalWire
- Username or email enumeration without additional impact
- Open redirects without demonstrated security impact
- Rate-limiting or brute-force concerns on non-authentication endpoints

SignalWire reserves the sole right to determine whether a finding falls within or outside of scope.

Rules of Engagement

To keep researchers, customers, and SignalWire safe during testing:

You must:

- Test only against systems explicitly listed as in scope
- Use only your own SignalWire account(s) for testing — never another customer's account, and never a SignalWire employee account
- Stop testing immediately and notify us if you encounter customer data, employee data, or other sensitive information
- Provide enough information to validate and reproduce the issue
- Give SignalWire a reasonable opportunity and time to remediate before publicly disclosing the issue
- Respect rate limits and not generate unreasonable load against our systems

You must not:

- Access, modify, exfiltrate, store, or destroy data belonging to SignalWire, our customers, or any third party
- Disrupt service availability for other users
- Use findings for personal gain, extortion, or any purpose other than the good-faith reporting contemplated by this policy
- Test using techniques that could damage SignalWire systems or customer data, including but not limited to denial-of-service attacks, automated brute force, large-scale data scraping, or destructive payloads
- Pivot from one in-scope system to another out-of-scope system or to internal infrastructure
- Submit findings on behalf of someone who has not agreed to this policy
- Publicly disclose the vulnerability before SignalWire has had a reasonable opportunity to remediate (typically 90 days from acknowledgment, unless a different timeline is communicated by SignalWire)

Inadvertent Access to Sensitive Data

If you inadvertently access, discover, or acquire SignalWire customer data, employee data, or other personal or sensitive information during research, you must:

1. Stop testing immediately and cease any activity that involves the data or the underlying vulnerability
2. Report the discovery to security@signalwire.com without delay
3. Not retain, copy, use, or disclose the data
4. Provide details of the inadvertent access in your submission

Use of Submitted Reports

By submitting a report under this policy, you grant SignalWire the right to use the contents of your report for any purpose, including disclosure as required by regulatory, contractual, or legal obligations. Submission of a report does not create a consumer, employment, or agency relationship between you and SignalWire.

Safe Harbor

To encourage good-faith security research and responsible disclosure, SignalWire will not pursue civil or criminal action, or refer the matter to law enforcement, for accidental or good-faith violations of this policy. We consider security research and vulnerability disclosure activities conducted consistent with this policy to be authorized conduct under the U.S. Computer Fraud and Abuse Act (CFAA), the Digital Millennium Copyright Act (DMCA), and other applicable computer-use laws.

If your security research involves the networks, systems, information, applications, products, or services of a third party (which is not SignalWire), we cannot bind that third party, and they may pursue legal action or notify law enforcement. We cannot and do not authorize security research in the name of any other entity, and we do not offer to defend, indemnify, or otherwise protect you from any third-party action arising from your research activities.

You are expected to comply with all laws applicable to you and to refrain from disrupting or compromising any data beyond what this policy permits.

SignalWire reserves the sole right to determine whether activity conducted under this policy was in good faith and within the scope of the policy. Activity that exceeds the scope of this policy, violates the rules of engagement, or is conducted in bad faith is not protected by this safe harbor and may be subject to legal action.

Proactively contacting us before engaging in any uncertain activity is a significant factor in our determination of whether a violation is accidental or in good faith.

Coordinated Disclosure Timeline

SignalWire follows a coordinated disclosure model with the following targets:

- **Acknowledgment of receipt:** within 48 hours of submission
- **Target remediation and public disclosure:** within 90 days of acknowledgment

Where remediation requires longer than 90 days due to complexity, upstream dependencies, or coordinated industry response, SignalWire will notify the reporting researcher of the revised timeline.

For vulnerabilities affecting upstream open-source dependencies (such as FreeSWITCH), the disclosure timeline is coordinated with the upstream project, which may extend the public disclosure date beyond 90 days.

Reporting

To report a vulnerability, contact us at **security@signalwire.com**.

Please include enough information to validate and reproduce the issue, including affected systems, steps to reproduce, and proof of concept where applicable. Indicate whether you would like to be credited publicly when the issue is disclosed.

We treat all submissions with confidentiality.

This policy may be updated at any time. The current version is published at [URL]. Activity is evaluated against the version of the policy in effect at the time the activity occurred.