Stalwart Labs takes the security of its software and services seriously. This Vulnerability Disclosure Policy sets out how to report a vulnerability, what you can expect from us, and the safe-harbour protections we provide to good-faith security researchers. The corresponding machine-readable file is published at /.well-known/security.txt in accordance with RFC 9116.

Scope

This policy applies to:

In scope:

- the Stalwart Mail and Collaboration Server, all currently supported versions (see Supported versions below);
- the official Docker images published by Stalwart Labs;
- the websites operated by Stalwart Labs Ltd: **stalw.art**, **license.stalw.art**, and **support.stalw.art**;
- documentation that, if followed, would lead to an insecure deployment.

Out of scope:

- third-party integrations, plugins, or forks not maintained by Stalwart Labs;
- vulnerabilities that require physical access to the server hosting Stalwart;
- social engineering of Stalwart staff, customers, or community members;
- denial-of-service or volumetric attacks;
- attacks that depend on already-compromised credentials, unless the vulnerability itself enables credential compromise;
- theoretical findings without a practical exploitation path;
- self-hosted deployments operated by third parties (please contact the operator of the deployment directly).

Supported versions

We provide security updates for the following versions of Stalwart:

Version	Supported	End of support
0.15.x	✅	TBD
0.14.x	✅	2026-06-08
0.13.x	✅	2026-03-31
< 0.13	❌	Ended

We support the current major version and one previous major version. We strongly encourage operators to keep their installation on a currently supported version.

How to report a vulnerability

Do not report security vulnerabilities through public GitHub issues, public discussions, the Support Portal, social media, or any other public channel. Public reports give attackers the time window between disclosure and patch release.

Use one of the following private channels:

1. **Email** (preferred): send the details to **security@stalw.art**. PGP encryption is available on request.
2. **GitHub private security advisory**: open a draft advisory in the relevant repository under github.com/stalwartlabs using the “Report a vulnerability” button on the Security tab.
3. **Backup**: if you have not received an acknowledgement within forty-eight (48) hours, follow up at **hello@stalw.art** referencing your earlier report.

What to include

To help us triage and address the issue quickly, please include:

Required:

- a clear description of the vulnerability and its category (for example, authentication bypass, server-side request forgery, memory corruption);
- the affected component and version, with commit hash where applicable;
- step-by-step reproduction instructions;
- an impact assessment (what could an attacker achieve, under what preconditions).

Helpful, where available:

- the configuration required to reproduce the issue;
- proof-of-concept code, scripts, or network captures (please redact any third-party data);
- relevant log excerpts;
- a suggested mitigation or fix.

Our response process

Timeline commitments:

- **Initial acknowledgement:** within twenty-four (24) hours of receipt.
- **Triage and detailed response:** within seventy-two (72) hours, including an initial severity assessment and the channel we will use for ongoing communication.
- **Status updates:** at least every seven (7) days until the issue is resolved.
- **Resolution target:** ninety (90) days from receipt for the majority of issues; longer for issues that require coordinated upstream changes.

What we will do:

1. Acknowledge your report and assign an internal tracking identifier.
2. Validate the vulnerability and assess its severity (using CVSS v3.1 unless otherwise specified).

3. Develop, test, and review the fix.
4. Coordinate the disclosure timeline with you, and with relevant upstreams or downstreams where applicable.
5. Release a security update and publish a security advisory through GitHub Security Advisories. Critical issues may receive an out-of-band release.
6. Credit you in the advisory by name or handle, unless you ask us not to (see Recognition).

Disclosure policy

We follow coordinated disclosure principles:

- **Default timeline:** ninety (90) days from your initial report to public disclosure.
- **Earlier disclosure:** may occur if the issue is being actively exploited in the wild, or if a coordinated industry-wide disclosure date applies.
- **Later disclosure:** may be necessary for complex issues that require significant code changes, downstream coordination, or operator preparation.
- **Pre-notification:** for severe issues, we may pre-notify operators of large Stalwart deployments under embargo so that patches can be applied before public disclosure.

Legal safe harbour

If you act in good faith and comply with this policy, Stalwart Labs Ltd and Stalwart Labs LLC will:

- **Not** initiate or support legal action against you in connection with your research;
- **Not** report your activity to law enforcement;

- **Not** suspend or terminate your access to the Services in connection with your research;
- consider your activity to be authorised conduct for the purposes of the UK Computer Misuse Act 1990, the U.S. Computer Fraud and Abuse Act (where applicable), and analogous laws of the country in which we operate the affected service;
- consider your activity to be authorised use for the purposes of any anti-circumvention provisions (such as section 1201 of the U.S. Digital Millennium Copyright Act).

To benefit from this safe harbour, you must:

- **Test only against your own Stalwart installation, or against a deployment operated by Stalwart Labs and explicitly designated as in scope.** Do not test against installations operated by third parties without the operator's authorisation.
- **Not access, modify, exfiltrate, or destroy data** belonging to Stalwart Labs or to any third party. If you incidentally observe data that is not your own, stop, do not retain it, and tell us in your report.
- **Not degrade the availability** of the Services. No volumetric, brute-force, or denial-of-service testing.
- **Not publicly disclose** the vulnerability before the agreed coordinated-disclosure date.
- Act in good faith and not for malicious purpose, extortion, or competitive advantage.

If you are unsure whether a given activity falls within this safe harbour, ask us at **security@stalw.art** before you proceed. We would rather have the conversation than read about it later.

This safe harbour does not authorise activity that violates the rights of third parties, even where it would otherwise be permitted under this policy.

Recognition

We believe in recognising security researchers who help keep Stalwart users safe:

- **Security advisory credit**: by default, we credit reporters in our published GitHub Security Advisories. Tell us if you would prefer to remain anonymous, or if you would like a specific name, handle, or organisation to appear.
- **Hall of fame**: significant contributions may be listed in our security acknowledgements.
- **Stalwart merchandise**: we may send swag for notable contributions.

We do not currently operate a paid bug bounty programme, and we are not affiliated with any third-party bounty platform. Beware of any communication that claims otherwise.

Security updates

Stay informed:

- Subscribe to GitHub Releases for the Stalwart server.
- Watch the GitHub Security Advisories page.
- Operators of the Stalwart Mail and Collaboration Server should monitor the relevant Docker image registry for updated tags.

Update process:

- Security updates are normally released as patch versions (for example, 0.15.1 → 0.15.2).
- Critical vulnerabilities may receive out-of-band releases.
- Docker images are updated at the same time as the source release.

Contact

- **Vulnerability reports: security@stalw.art**

- **General security questions: hello@stalw.art**
- **PGP key:** available on request to **security@stalw.art**.
- **Postal address:** Stalwart Labs Ltd, Attn: Security, 128 City Road, London EC1V 2NX, United Kingdom.

Changes to this policy

We may update this Vulnerability Disclosure Policy from time to time. The current version is dated at the top of this page. The accompanying /.well-known/security.txt file lists the current policy URL and an `Expires` date in accordance with RFC 9116; we refresh that file before its expiry.