Report a suspected vulnerability

Send a responsible, minimally invasive vulnerability report through the dedicated security route.

Task: Use the report a suspected vulnerability process consistently and retain the right evidence.

Audience: Security researchers, customers and partners

Owner: Obedience Governance

Version 2026.08 | Reviewed 2026-08-22 | Next review 2027-02-22

Purpose and scope

Send a responsible, minimally invasive vulnerability report through the dedicated security route.

Use this guide as orientation, then rely on the signed agreement, current policy or named support response where those sources set a more specific obligation.

Prepare the right information

- Affected host and safe reproduction summary.
- Potential impact without unnecessary exploitation.
- Researcher contact and disclosure preference.

Follow the controlled process

1. Frame the need

State the desired outcome, affected product and accountable contact. For report a suspected vulnerability, avoid assumptions that have not been confirmed in writing.

2. Review and decide

Use the current governed source, record material questions and obtain approval from the person who owns the decision.

3. Retain evidence

Keep the final reference, date, decision and any follow-up action together so a later reviewer can reconstruct what happened.

Expected record

- A timestamped security report.
- Acknowledgement and triage.
- A coordinated follow-up path.

Keep in mind

Do not access unrelated data, persist access, degrade service, phish users or publish details before coordination.

Security and disclosure boundary

- Never send passwords, authentication codes, private keys or recovery codes to Obedience staff.
- Share the minimum customer, project and commercial information needed for the stated purpose.
- Public documentation explains controls and responsibilities without publishing exploitable topology, credentials or confidential implementation detail.