



admin@tuwa.io

Security Policy

Last Updated: October 14, 2026

This Security Policy explains how to report a security vulnerability in the TUWA ecosystem, what you can expect from FOP Tkach Oleksandr ("we," "us," or "our") when you do, and who is responsible for what. It covers our open-source npm packages, Quasar Cloud, Quasar Community Edition and Quasar Payments. We welcome reports from security researchers and users, and we will not take legal action against research done in good faith under this policy (Section 5).

1. What We Promise and What We Do Not

- **We promise** to answer reports within the times in Section 6, to keep you informed until the issue is resolved, not to pursue good-faith research (Section 5), and to thank you publicly if you wish.
- **We do not promise** that our software or services are free of vulnerabilities, that we pay rewards (there is no bug bounty program, see Section 7), or that we fix versions that are no longer supported (Section 2).

2. Scope

In scope:

- The latest published versions of our npm packages (@tuwaio/*).
- Quasar Cloud: api.tuwa.io and the dashboard at quasar.tuwa.io.
- The code of Quasar Community Edition, latest minor version.
- Quasar Payments, from its release: the payment engine, the checkout API and checkout tokens, the hosted payment page (/pay), the EIP-3009 relayer, the ERC-7677 paymaster proxy, the ERC-7715 auto-charge collector, payments.v1 webhooks and verifyWebhook, the payment ledger and issued documents, @tuwaio/nova-payments and @tuwaio/quasar-sdk/checkout.

Examples that are always in scope: access to another organization's apps, transactions or keys; a forged or replayed webhook signature; a package that exposes a key or signs something the user did not confirm. From the release of Quasar Payments, also: a payment counted for another invoice or from another payer; a changed amount, asset, network or recipient of a quote; a bypass of AML screening; access to another person's invoice through its token or by guessing; a change to the ledger or a document that the hash-chain check does not detect; a charge above the limit or outside the period of a wallet permission; a relayer or paymaster that pays gas for someone else's calls.

Out of scope:

- Quasar Community Edition installations run by others: please report to their operator (a vulnerability in the code of Community Edition itself is in scope).
- Third-party services, including wallets, RPC providers, WalletConnect, GoPlus, Chainalysis, Pimlico and other paymasters, Gelato and Resend. Please report to them directly.
- The content of sanctions lists, such as the OFAC list.
- Reports without a demonstrated impact, such as missing security headers, version banners or the absence of rate limits on non-sensitive pages.
- Social engineering and physical access.

3. How to Report

Email security@tuwa.io with:

- the package and version, or the service and route, that is affected;
- the steps to reproduce or a proof of concept;
- the impact you believe it has.

Please do not disclose the vulnerability publicly until it is fixed, until a disclosure date we have agreed on, or, if we could not agree, until the written notice period in Section 6 has passed. Please do not send us personal data of others beyond what is needed to show the issue.

4. Rules for Testing

- Test only with your own accounts and apps, in test mode and on test networks. If a vulnerability cannot be demonstrated there, report the suspected issue without conducting unauthorized production testing.
- Do not access, change or move funds or data that are not yours. If you reach them by accident, stop, tell us, and delete what you obtained.
- No load testing, denial of service, spam, or automated scanning beyond the API rate limits.
- No social engineering or phishing of our team, our users or our providers.
- Follow the laws that apply to you.

5. Safe Harbor

If you make a good-faith effort to follow this policy, we consider your research authorized on systems we own and control, within the limits in Sections 2 and 4. We will work with you to understand and fix the issue, and we will not bring legal action or report you to law enforcement for that research. If a third party brings legal action against you for research that followed this policy, we will make it known that your research was authorized by us. This protection does not cover actions that break the rules in Section 4 or systems that are not ours; we cannot authorize activity on third-party systems.

6. How We Respond

- **Acknowledgement:** within 3 business days.
- **Assessment:** within 7 business days, with our view of severity.
- **Updates:** at least every 14 days until the issue is resolved.
- **Fix targets** by CVSS 4.0 severity: critical — 7 days, high — 30 days, medium — 90 days, low — when possible. Any threat to funds is treated as critical.

- **Disclosure:** we aim to coordinate disclosure with you after a fix. If the risk to users requires action before a fix, we may agree with you on an earlier advisory that describes the risk and the steps users can take. If the issue remains unresolved 90 days after the report, we will discuss the disclosure date and risk-mitigation steps with you; if we cannot agree, either of us may publish after giving the other 30 days' written notice, without details that would let others exploit the issue. For our packages and Quasar Community Edition we publish a GitHub Security Advisory and request a CVE where appropriate. If you wish, we credit you in the advisory.

7. Rewards

This policy does not promise rewards, and we do not run a bug bounty program. If we start one, it will have its own terms with the amounts. Any reward would be paid only for reports that follow this policy, never to persons under sanctions, and the recipient is responsible for their own taxes.

8. Shared Responsibility

- **We** are responsible for the code of our packages and of Quasar Community Edition, and for operating Quasar Cloud.
- **Quasar Cloud customers** are responsible for their API keys, webhook secrets, the provider keys and RPC endpoints they set up, and the access of their team members; from the release of Quasar Payments, also for their recipient addresses, AML and gasless settings.
- **Operators of Quasar Community Edition** are responsible for their deployment, updates, secrets, RPC providers, backups and infrastructure.
- **Buyers and users** are responsible for their wallets and keys, and for checking what they sign.
- **Third-party services** are responsible for their own security.

TUWA is non-custodial: we never hold your private keys or funds, and we cannot reverse a transaction on a blockchain.

9. What We Do to Stay Secure

We keep dependencies up to date, publish npm releases with provenance, require two-factor authentication and least-privilege access in our organization, encrypt stored secrets, keep an append-only, hash-chained ledger for Quasar Payments, monitor our services and show their status at status.tuwa.io, and follow an incident response plan. This describes our practices; it is not a guarantee.

10. Incident Notifications

If a security incident affects Quasar Cloud customers, we notify them without undue delay. If personal data is breached, we notify the supervisory authority and the affected people as data protection law requires. Under the GDPR, where authority notification is required, it must be made without undue delay and, where feasible, within 72 hours after becoming aware of the breach; communication to individuals is required without undue delay where the breach is likely to result in a high risk to their rights and freedoms, subject to statutory exceptions (Regulation (EU) 2016/679, Articles 33 and 34). Outages are shown at status.tuwa.io.

11. Disclaimers

This policy is not a contract and not a warranty. Our software is provided "as is" under its license (Apache-2.0 for our packages and Quasar Community Edition, MIT-0 for the starter templates). Limitation of liability and governing law are set out in our [Terms of Service](#). We may change this policy; the date of the current version is at the top.

12. Contact

Report vulnerabilities to security@tuwa.io. For other questions about this policy, please contact us at admin@tuwa.io.