SECURITY AUDIT REPORT

Beldex Network Security Audit

Full-Stack Security Audit

Report date: September 2026

Engagement: Full-stack independent security audit

Codebase: Beldex network, production release `v7.0.3`

Release verified: `v7.0.3` production release tag

PREPARED FOR

BELDEX

PREPARED BY

DR DAKARA RESEARCH
SECURITY & PROTOCOL AUDITS

Summary

The Beldex network's core trust properties hold under direct attack. That is the finding of a source-level security audit by Dakara Research, conducted from June to September 2026, covering the full stack: the core daemon; the command-line wallet and the wallet core shared by the desktop and mobile clients; the Belnet onion-routing layer; the message storage server; the wallet applications; and the BChat messenger.

The areas an adversary would most want to break were attacked directly and held: the transaction and privacy cryptography, the authentication and authorization model, and the integrity of consensus and storage. Defects that were found were remediated and independently re-verified against the shipped code.

Every Critical finding is resolved in the production `v7.0.3` release.

The engagement

Dakara Research performs independent security and protocol audits for cryptocurrency networks. This engagement was scoped to the whole Beldex stack rather than a single component, and ran across several months rather than a single pass, so the network could be examined the way a determined adversary would examine it: end to end, across every trust boundary, and with time to follow attack paths that a short review cannot.

The methodology combined line-by-line source review with adversarial validation of every material finding, proof-of-concept confirmation of the highest-impact issues, and a final re-verification stage in which each shipped fix was re-checked against the deployed release to confirm it resolved its issue without introducing a new one. Findings were held to a high evidentiary bar: each was independently corroborated and checked against the surrounding code for existing mitigations before it was reported.

Scope, by component:

- **Core daemon:** consensus and transaction validation, the peer-to-peer layer, the RPC surface, and the masternode and staking logic.
- **Wallets:** the command-line wallet and the wallet core, including multisig, key handling, and the trust boundary against a remote node.
- **Belnet:** the onion-routing transport derived from Lokinet.
- **Storage server:** the always-online service that holds messages for offline clients, including its authentication, authorization, and storage-integrity model.
- **Applications:** the desktop and mobile wallet applications and the BChat messenger.

Results at a glance

Severity	Count	Status
Critical	5	**All resolved and re-verified**
High	8	Resolved, two with fixes delivered and awaiting a tagged release
Medium	14	Resolved / remediation delivered
Low	25	Addressed, or accepted with documented rationale
Informational	12	Hardening guidance provided

Low and Informational counts reflect grouped items; per-finding detail is in the milestone reports delivered privately to Beldex. Every Critical and High finding was accompanied by a review-ready fix.

The Critical findings are the ones that matter most to a network's users, and each is now closed:

- A coinbase and governance reward validation gap, closed in the network's hard fork and confirmed active in production.
- A remote masternode crash in the daemon, fixed and merged.
- A pre-authentication heap overflow in the daemon, fixed and merged.
- A multisig secret-share extraction in the wallet, closed by rejecting the nonce-reuse condition it depended on.
- A remote overflow in a public RPC handler, closed by an unconditional length bound.

What held

An audit report is often read only for what broke. For a network's users, what held is just as important. Dakara Research attacked the following directly, and they held:

- **Fund safety.** No path to theft or creation of funds. The RingCT, ring-signature, and Bulletproofs+ cryptography is sound, as are the balance and double-spend checks that protect the money supply.

- **Privacy.** Signature verification cannot be bypassed. The onion and channel cryptography on the message-storage path is authenticated, with fresh nonces and replay binding throughout.
- **Authentication and authorization.** No SQL injection, no authentication or authorization bypass, and correctly scoped subaccount delegation on the storage server. No privileged daemon RPC action is reachable from the public interface.
- **Wallet integrity.** No forgeable payment, spend, or reserve proof; a sound trust boundary against a malicious remote node; and correct hardware-wallet signing integrity.

These are the properties the network's trust model rests on, and they are the substantive positive result of the audit.

Findings and remediation

It is not enough to report a fix; a fix must be confirmed against the code that actually ships. Each remediation was re-checked against the deployed `v7.0.3` release to confirm it resolved its issue without introducing a regression. As of that release:

- **All five Critical findings are resolved and re-verified in production.**
- The High and Medium findings are resolved, with two daemon items (a peer-triggerable resource-exhaustion pair and a set of public-RPC rate caps) awaiting a tagged release: the fixes are prepared and delivered.
- Lower-severity items were addressed or accepted with documented rationale, and hardening guidance was provided for the informational tier.

Dakara Research will re-verify the two remaining fixes when they ship in a tagged release and issue final clearance at that time.

Limitations

A security audit is a point-in-time assessment. It identifies issues discoverable within the engagement's scope and schedule and does not constitute a guarantee that the reviewed software is free of vulnerabilities. This audit covered the components and releases named above; code that changes after this review, and components outside the stated scope, should be assessed separately. Findings should be remediated and re-verified, and this report describes the state of the code as of the `v7.0.3` release.

Conclusion

The Beldex network submitted to a thorough, independent, full-stack security audit and came through it with its core trust properties intact and every Critical finding resolved and re-verified in production. The defects that were found were well-characterized and remediated. This is the profile of a network with the engineering discipline to act on independent findings.

About Dakara Research

Dakara Research is an independent security and protocol audit practice for cryptocurrency networks. Our work pairs line-by-line source review with adversarial validation, proof-of-concept confirmation, and re-verification against shipped code, so that a clean result means the network was genuinely tested, not merely reviewed.

Dakara Research, dakara-research.com