TRIBYTE

U3 PROTOCOL

SECURITY AUDIT REPORT

SEPTEMBER 2025

Every Byte Builds Immutable Trust

No. 202509080002

Contents

Summary

Executive Summary

U3 conducted a comprehensive security audit of its deposit contracts in August 2025. The U3 Protocol enables users to deposit funds on the blockchain into a bank account. The contract is minimal and non-custodial, reducing certain attack classes. The audit aimed to identify vulnerabilities and ensure the robustness of the codebase. It covered both core contracts and their dependencies, providing a thorough evaluation of the project's security posture.

The assessment leveraged a dual methodology, combining Manual Review and Static Analysis to meticulously examine the contracts. Our team adopted a multifaceted testing strategy, integrating black-box, gray-box, and white-box techniques to simulate real-world attack scenarios and detect potential weaknesses. Black-box testing evaluated the contracts from an external attacker's perspective, gray-box testing probed internal behaviors using specialized scripting tools, and white-box testing featured an in-depth, line-by-line code review by our experts.

Project Summary

Project Name	U3 Protocol
Language	Rust
Github Link	https://github.com/u3com/u3-deposit-sol
Commit Hash	1022476d6e541e6c46bad583482e5aa1c4424987

Vulnerability Summary

Severity Level	Summary
Critical	0
High	0
Medium	0
Low	0
Informational	3

Findings

[CD-01] Missing deposit identifier exposure in event

Category	Contract Design
Severity	Informational
Location	programs/u3-deposit/src/lib.rs

Description

The *UsdtDeposited* event is missing a deposit identifier, which necessitates off-chain ordering assumptions for index reconstruction. Adding the deposit identifier to the event is a a good practice for traceability, idempotency, and off-chain indexing. It will simplify off-chain operations by:

1. Ensuring that no deposits are missed by verifying the order of *depositId*.
2. Preventing the indexing of duplicate events.

Recommendation

Add a Global sequential counter (pool.deposit_count) to the event for reliable correlation.

[PD-01] Privacy and Compliance Risk with Public Email Exposure

Category	Protocol Design
Severity	Informational
Location	programs/u3-deposit/src/lib.rs

Description

Emails are currently emitted in events and are permanently public, posing privacy and compliance risks, including potential GDPR violations.

Recommendation

Store a hashed version of the email (e.g., sha256(email)) and emit the hash instead. Keep raw emails off-chain. If access to the raw email is necessary, use off-chain storage anchored by the hash.

[CD-02] Missing Zero / Sanity Checks for New Admin & Recipient

Category	Contract Design
Severity	Informational
Location	programs/u3-deposit/src/lib.rs

Description

transfer_admin and *update_recipient* allow setting default / program / system program addresses inadvertently.

Recommendation

Add a check for the new pubkey and optionaly forbid program ID / system program.

Appendix

Vulnerability Fix Status

Status	Description
Resolved	The project team has successfully implemented a complete fix to address the vulnerability, eliminating the associated risks. All identified issues have been rectified, and the codebase has been updated to ensure the vulnerability no longer poses a threat.
Mitigated	The project team has taken steps to reduce the impact or likelihood of the vulnerability being exploited, but the issue has not been completely resolved. While the risk has been partially addressed, some potential exposure may still remain, and further action is recommended.
Acknowledged	The project team has reviewed and confirmed the existence of the vulnerability but has chosen not to address or mitigate it at this time. This status indicates awareness of the issue, and the team may accept the associated risks or plan to address it in the future.
Declined	The project team has reviewed the reported vulnerability but determined it does not require action, either because they believe it poses no significant risk to the project or because it falls outside the project's scope or priorities. The issue remains unaddressed, and the associated risks are accepted by the team.

Vulnerability Severity Level

Level	Description
Critical	Critical severity vulnerabilities pose an immediate and severe threat to the project's security, potentially leading to significant loss of funds, unauthorized access, or complete system compromise. These issues must be addressed urgently before deployment or continued operation to ensure the safety of users and the integrity of the project.
High	High severity vulnerabilities can substantially impact the project's functionality, potentially enabling exploitation that results in loss of assets, data breaches, or disruption of critical operations. It is strongly recommended to prioritize and resolve these issues promptly to mitigate risks.
Medium	Medium severity vulnerabilities may affect the project's performance or security under specific conditions, potentially leading to inefficiencies, minor exploits, or degraded user experience. It is advisable to address these issues to enhance the overall robustness of the system.
Low	Low severity vulnerabilities have a minimal impact on the project's security or functionality and are unlikely to be exploited in typical scenarios. However, they may still pose theoretical risks. The project team should evaluate these issues and consider fixing them to improve long-term stability.
Informational	Informational findings do not directly impact the security or functionality of the project but highlight areas for improvement, such as adherence to best practices, code optimization, or architectural enhancements. Addressing these suggestions can lead to better maintainability and alignment with industry standards.

Audit Items

Categories	Audit Items
Coding Convention	Obsolete Code
	Debug Code
	Comments / Dev Notes
	Compiler Versions
	License Identifier
	Require / Revert / Assert Usage
	Contract Size

	Gas Consumption
	Event Emission
	Parameter Check
General Vulnerability	Centralization
	Denial of Service
	Reply Attack
	Reentrancy Attack
	Race Conditions
	Integer Overflow / Underflow
	Arithmetic Accuracy Deviation
	Array Index Out of Bounds
	Receive / Fallback Function
	Payable and msg.value Usage
	tx.origin Authentication
	ERC20 Token Decimals
	ERC20 Safe Transfer
	ERC721 Safe Transfer
	Rebasable Token Support
	Native Token Support
	Storage / Memory Usage
	Function Permissions
External Dependency	Oracle Usage
	External Protocol Interaction
Protocol Design	Economics Design
	Formula Derivation
Contract Design	Factory Contract

	Proxy Usage
	EIP2535 Diamond Pattern Usage
	Upgradability / Pluggability

Disclaimer

Tribyte issues this audit report based solely on the code and materials provided by the client up to the report’s issuance date. We assume the provided information is complete, accurate, and untampered. Tribyte is not liable for any losses or issues arising from incomplete, altered, or concealed information, or from changes made after the audit.

This report evaluates only the specified smart contracts or systems within the agreed scope, using Tribyte’s tools and methodologies. It does not endorse the project’s business model, team, or legal status, nor does it guarantee the absence of vulnerabilities due to technical limitations. The report is for the client’s use only and may not be shared, quoted, or relied upon by third parties without Tribyte’s written consent.

Conclusion

During this security audit, we conducted a comprehensive examination of the U3 Protocol's smart contract design and implementation. Our assessment encompassed multiple security dimensions: we thoroughly reviewed all external dependencies (including mathematical libraries, role management systems, and other common vulnerability vectors) and identified no security concerns in these foundational components. We then analyzed the protocol's design documentation to gain a thorough understanding of the deposit mechanism and its underlying architecture. Subsequently, we evaluated coding practices, business logic implementation, and overall security posture. Based on our comprehensive review, no major security vulnerabilities were identified, and the current deployment demonstrates adherence to industry best practices and security standards. As outlined in the Disclaimer section, we welcome constructive feedback and suggestions regarding our findings, audit procedures, and scope of examination.