GA GUARDIAN

USDT0

Superchain Deployment

Security Assessment

March 28th, 2025

Summary

Audit Firm Guardian

Prepared By Owen Thurm, Roberto Reigada, Daniel Gelfand

Client Firm USDT0

Final Report Date March 28, 2025

Audit Summary

USDT0 engaged Guardian to review the security of their USDT Superchain deployment. From the 17th of March to the 18th of March, a team of 3 auditors reviewed the source code in scope. All findings have been recorded in the following report.

For a detailed understanding of risk severity, source code vulnerability, and potential attack vectors, refer to the complete audit report below.

Table of Contents

Project Overview

Project Summary

Project Name	USDT0
Language	Solidity
Codebase	https://github.com/Everdawn-Labs/usdt0-tether-contracts-hardhat https://github.com/Everdawn-Labs/usdt0-oft-contracts
Commit(s)	Initial commit(s): 75e33fd404743d9548d2e8522f0f7e4ad468966f : 38a358a8451ccac9e11eb8446ff01663435c3bd5

Audit Summary

Delivery Date	March 28, 2025
Audit Methodology	Static Analysis, Manual Review, Test Suite, Contract Fuzzing

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Low	0	0	0	0	0	0
Info	4	0	0	1	0	3

Audit Scope & Methodology

Vulnerability Classifications

Severity	Impact: *High*	Impact: *Medium*	Impact: *Low*
Likelihood: *High*	🔴 Critical	🟠 High	🟡 Medium
Likelihood: *Medium*	🟠 High	🟡 Medium	🟢 Low
Likelihood: *Low*	🟡 Medium	🟢 Low	🟢 Low

Impact

High Significant loss of assets in the protocol, significant harm to a group of users, or a core functionality of the protocol is disrupted.

Medium A small amount of funds can be lost or ancillary functionality of the protocol is affected. The user or protocol may experience reduced or delayed receipt of intended funds.

Low Can lead to any unexpected behavior with some of the protocol's functionalities that is notable but does not meet the criteria for a higher severity.

Likelihood

High The attack is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount gained or the disruption to the protocol.

Medium An attack vector that is only possible in uncommon cases or requires a large amount of capital to exercise relative to the amount gained or the disruption to the protocol.

Low Unlikely to ever occur in production.

Audit Scope & Methodology

Methodology

Guardian is the ultimate standard for Smart Contract security. An engagement with Guardian entails the following:

- Two competing teams of Guardian security researchers performing an independent review.
- A dedicated fuzzing engineer to construct a comprehensive stateful fuzzing suite for the project.
- An engagement lead security researcher coordinating the 2 teams, performing their own analysis, relaying findings to the client, and orchestrating the testing/verification efforts.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts. Comprehensive written tests as a part of a code coverage testing suite.
- Contract fuzzing for increased attack resilience.

Findings & Resolutions

ID	Title	Category	Severity	Status
I-01	Old Signed Permits Will Be Invalid	Configuration	Info	Acknowledged
I-02	Hardcoded Etherscan API Keys	Best Practices	Info	Resolved
I-03	Missing LayerZero Configs For Optimism And Unichain	Configuration	Info	Resolved
I-04	DVNs For USDT Are Not Deployed Yet	Documentation	Info	Resolved

I-01 | Old Signed Permits Will Be Invalid

Category	Severity	Location	Status
Configuration	Info	TetherTokenOFTExtension.sol, OFTExtension.sol	Acknowledged

Description

Calling the `updateNameAndSymbol` function changes the token's name, which directly impacts the calculation of the `EIP712` domain separator. Because the domain separator relies on the token name, previously signed permits become invalid after this function is executed.

Recommendation

Clearly document that previously issued signed permits will be invalidated when calling `updateNameAndSymbol`. Additionally, inform token holders in advance to avoid confusion or disruptions.

Resolution

USDT0 Team: Acknowledged.

I-02 | Hardcoded Etherscan API Keys

Category	Severity	Location	Status
Best Practices	Info	hardhat.config.ts	Resolved

Description

The `hardhat.config.ts` file contains hard-coded references to multiple Etherscan API keys.

Recommendation

Update your `hardhat.config.ts` to securely retrieve Etherscan API keys from environment variables. For example: `apiKey: process.env.UNICHAIN_ETHERSCAN_KEY`.

Resolution

USDT0 Team: Resolved.

I-03 | Missing LayerZero Configs For Optimism And Unichain

Category	Severity	Location	Status
Configuration	Info	layerzero-prod.config.ts	Resolved

Description

The file layerzero-prod.config.ts contains the `LayerZero` configurations for various USDT contracts deployed across the supported blockchains. However, configurations for Unichain and Optimism are currently missing from this file.

Recommendation

Add the necessary `LayerZero` configurations for Unichain and Optimism to ensure comprehensive coverage and proper integration across all the supported blockchains.

Resolution

USDT0 Team: Resolved.

I-04 | DVNs For USDT Are Not Deployed Yet

Category	Severity	Location	Status
Documentation	Info	Global	Resolved

Description

Currently, there are no Data Verification Nodes (DVNs) deployed on Optimism and Unichain, as stated in the official LayerZero deployment documentation: https://docs.layerzero.network/v2/deployments/dvn-addresses.

Recommendation

Coordinate with the LayerZero team to either deploy DVNs on these networks or obtain an update on their planned timeline for deployment.

Resolution

USDT0 Team: Resolved.

Disclaimer

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Guardian to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Guardian’s position is that each company and individual are responsible for their own due diligence and continuous security. Guardian’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by Guardian is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

Notice that smart contracts deployed on the blockchain are not resistant from internal/external exploit. Notice that active smart contract owner privileges constitute an elevated impact to any smart contract’s safety and security. Therefore, Guardian does not guarantee the explicit security of the audited smart contract, regardless of the verdict.

About Guardian Audits

Founded in 2022 by DeFi experts, Guardian Audits is a leading audit firm in the DeFi smart contract space. With every audit report, Guardian Audits upholds best-in-class security while achieving our mission to relentlessly secure DeFi.

To learn more, visit https://guardianaudits.com

To view our audit portfolio, visit https://github.com/guardianaudits

To book an audit, message https://t.me/guardianaudits