GA GUARDIAN

USDT0

Flare Deployment

Security Assessment

July 16th, 2025

Summary

Audit Firm Guardian

Prepared By Owen Thurm, Daniel Gelfand

Client Firm USDT0

Final Report Date July 16, 2025

Audit Summary

USDT0 engaged Guardian to review the security of their USDT0's deployment on Flare. From the 7th of March to the 8th of March, a team of 2 auditors reviewed the source code in scope. All findings have been recorded in the following report.

Confidence Ranking

Given the lack of critical issues detected and minimal code changes following the main review, Guardian assigns a Confidence Ranking of 5 to the protocol. Guardian advises the protocol to consider periodic review with future changes. For detailed understanding of the Guardian Confidence Ranking, please see the rubric on the following page.

🔗 Blockchain network: **Flare**

✅ Verify the authenticity of this report on Guardian's GitHub: https://github.com/guardianaudits

Guardian Confidence Ranking

Confidence Ranking	Definition and Recommendation	Risk Profile
5: Very High Confidence	Codebase is mature, clean, and secure. No High or Critical vulnerabilities were found. Follows modern best practices with high test coverage and thoughtful design. **Recommendation:** Code is highly secure at time of audit. Low risk of latent critical issues.	0 High/Critical findings and few Low/Medium severity findings.
4: High Confidence	Code is clean, well-structured, and adheres to best practices. Only Low or Medium-severity issues were discovered. Design patterns are sound, and test coverage is reasonable. Small changes, such as modifying rounding logic, may introduce new vulnerabilities and should be carefully reviewed. **Recommendation:** Suitable for deployment after remediations; consider periodic review with changes.	0 High/Critical findings. Varied Low/Medium severity findings.
3: Moderate Confidence	Medium-severity and occasional High-severity issues found. Code is functional, but there are concerning areas (e.g., weak modularity, risky patterns). No critical design flaws, though some patterns could lead to issues in edge cases. **Recommendation:** Address issues thoroughly and consider a targeted follow-up audit depending on code changes.	1 High finding and ≥ 3 Medium. Varied Low severity findings.
2: Low Confidence	Code shows frequent emergence of Critical/High vulnerabilities (~2/week). Audit revealed recurring anti-patterns, weak test coverage, or unclear logic. These characteristics suggest a high likelihood of latent issues. **Recommendation:** Post-audit development and a second audit cycle are strongly advised.	2-4 High/Critical findings per engagement week.
1: Very Low Confidence	Code has systemic issues. Multiple High/Critical findings (≥5/week), poor security posture, and design flaws that introduce compounding risks. Safety cannot be assured. **Recommendation:** Halt deployment and seek a comprehensive re-audit after substantial refactoring.	≥5 High/Critical findings and overall systemic flaws.

Table of Contents

Project Overview

Project Summary

Project Name	USDT0
Language	Solidity
Codebase	https://github.com/Everdawn-Labs/usdt0-tether-contracts-hardhat and https://github.com/Everdawn-Labs/usdt0-oft-contracts
Commit(s)	Initial commit(s): 675d3a0df1d9823420586f99e8fb007f2d721ae9 and 7d7af3a5bb828d18edd0f1901ca2bbe27bf6243d
Addresses	OFT Proxy: 0x567287d2A9829215a37e3B88843d32f9221E7588 OFT Implementation: 0x767F94783B3Ca9eC74807932d3FeB3c5010B9c89 OFT Proxy Admin: 0xa882c21c9df00958a958cde96f2b2ae8fb4315b1 USDT0 Proxy: 0xe7cd86e13ac4309349f30b3435a9d337750fc82d USDT0 Implementation: 0x779ded0c9e1022225f8e0630b35a9b54be713736 USDT0 Proxy Admin: 0xb8ce59fc3717ada4c02eadf9682a9e934f625ebb

Audit Summary

Delivery Date	July 16, 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

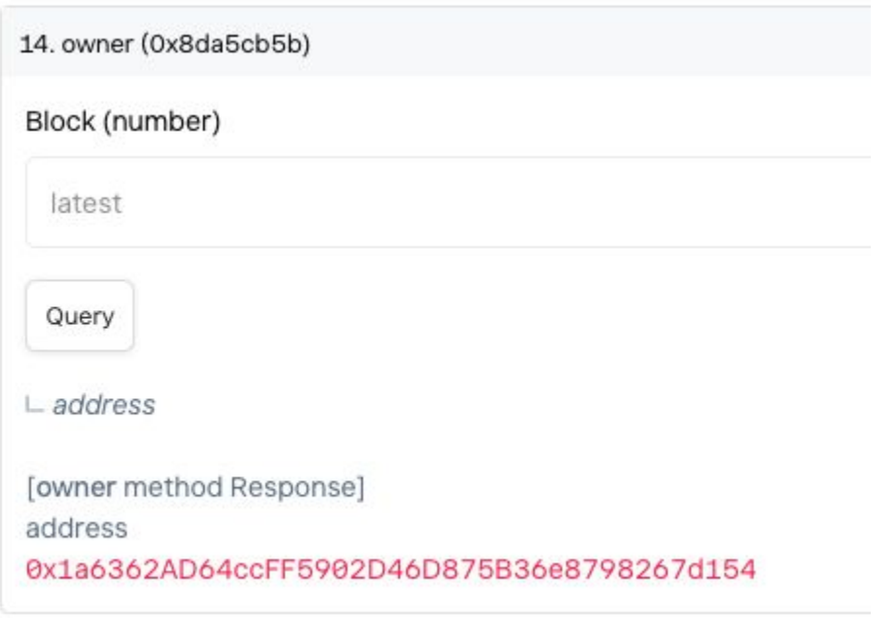
ID	Title	Category	Severity	Status
I-01	Incorrect USDT0 Owner	Configuration	Info	Resolved
I-02	oftContract Unassigned	Configuration	Info	Resolved
I-03	Incorrect ProxyAdmin Owner	Configuration	Info	Resolved
I-04	Safe Signer Change	Configuration	Info	Acknowledged

I-01 | Incorrect USDT0 Owner

Category	Severity	Location	Status
Configuration	Info	Global	Resolved

Description

The owner of the `USDT0` token on Flare is an EOA rather than the multisig address of `0x6ae078461f35c3cC216A71029F71ee7Bc4d9a10b`



Recommendation

Transfer ownership on the `USDT0` token from `0x1a6362AD64ccFF5902D46D875B36e8798267d154` to the safe address of `0x6ae078461f35c3cC216A71029F71ee7Bc4d9a10b`.

Resolution

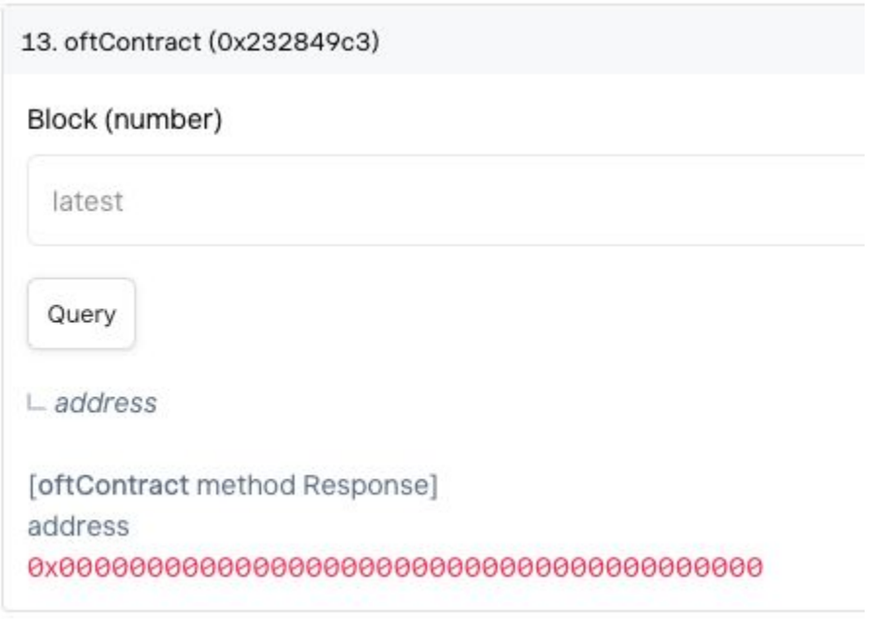
USDT0 Team: Resolved.

I-02 | oftContract Unassigned

Category	Severity	Location	Status
Configuration	Info	Global	Resolved

Description

The `oftContract` on the `USDT0` contract is assigned to the zero address.



Recommendation

Assign the `oftContract` to the OFT address of `0x567287d2A9829215a37e3B88843d32f9221E7588`.

Resolution

USDT0 Team: Resolved.

I-03 | Incorrect ProxyAdmin Owner

Category	Severity	Location	Status
Configuration	Info	Global	Resolved

Description

The proxy admin for both the OFT contract and the USDT0 contract is assigned to an EOA rather than the multisig address of `0x6ae078461f35c3cC216A71029F71ee7Bc4d9a10b`.

See the following failing tests:

https://github.com/Everdawn-Labs/usdt0-oft-contracts/blob/4f0f8f821676056a08120a4b72b0ff74aefdefef/test/foundry/USDT0ForkTests.t.sol#L373

https://github.com/Everdawn-Labs/usdt0-oft-contracts/blob/4f0f8f821676056a08120a4b72b0ff74aefdefef/test/foundry/USDT0ForkTests.t.sol#L379

Recommendation

Transfer ownership of the proxy admin contracts to the multisig address of `0x6ae078461f35c3cC216A71029F71ee7Bc4d9a10b`.

Resolution

USDT0 Team: Resolved.

I-04 | Safe Signer Change

Category	Severity	Location	Status
Configuration	Info	Global	Acknowledged

Description

The signers for the USDT0 Multisig on Ethereum are as follows:

[0x00F6D2b4B69Ce697f913Da16A9D73283dc4C78F2,
[0x4192D72c281dB0eF10464dD274EE583C33256ac5,
[0x7D8e979dcC6EC933c70FBe28B2B7700907D2aFEA,
[0x5F0DcA105195Bd58277aa4b4CABC90a791E1b982,
[0x488A3d37442F583c1c0a356118d1d6181b22434c]

However the signers for the USDT0 Multisig on Flare are the following:

[0x1a6362AD64ccFF5902D46D875B36e8798267d154,
0x4192D72c281dB0eF10464dD274EE583C33256ac5,
0x7D8e979dcC6EC933c70FBe28B2B7700907D2aFEA,
0x5F0DcA105195Bd58277aa4b4CABC90a791E1b982,
0x488A3d37442F583c1c0a356118d1d6181b22434c]

These list of signers differ by one signer, the address 0x00F6D2b4B69Ce697f913Da16A9D73283dc4C78F2 on ETH has been replaced by 0x1a6362AD64ccFF5902D46D875B36e8798267d154 on the Flare Multisig.

Recommendation

Confirm if the difference in signers is intentional or not. If it is not then correct the signer difference.

Resolution

USDT0 Team: Acknowledged.

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

Founded in 2022 by DeFi experts, Guardian is a leading audit firm in the DeFi smart contract space. With every audit report, Guardian 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