

USDT0 · SECURITY REVIEW

USDT0

Conflux Deployment, USDT0 and CNHT0.

A security review of Conflux Deployment, USDT0 and CNHT0.

CLIENT	PROJECT	AUDITORS	AUDIT WINDOW	FINAL REPORT
USDT0	Conflux Deployment, USDT0 and CNHT0	Guardian	October 30 – November 10, 2025	November 10, 2025

§ 00

Contents.

15 pages: overview, confidence ranking, scope, 7 findings, disclaimer, and about Guardian.

§ 01	Overview	P. 03
§ 02	Confidence Ranking	P. 04
§ 03	Scope & Classifications	P. 05
§ 04	Findings	P. 06
	Main Review · 6 findings	P. 07
	Remediation Review · 1 finding	P. 13
§ 05	Disclaimer	P. 14
§ 06	About Guardian	P. 15

§ 01

Overview.

Guardian reviewed Conflux Deployment, USDT0 and CNHT0 across 2 review rounds. The final report includes 1 Medium, 4 Low, 2 Informational findings.

AUDIT FIRM	REPOSITORY
Guardian	https://github.com/Everdawn-Labs/usdt0-oft-contracts , https://github.com/Everdawn-Labs/usdt0-tether-contracts-hardhat
CLIENT	METHODOLOGY
USDT0	Smart contract · Manual · Main Review · Remediation Review
PROJECT	
Conflux Deployment, USDT0 and CNHT0	
PREPARED BY	
Guardian	
AUDIT WINDOW	
October 30 – November 10, 2025	
FINAL REPORT	
November 10, 2025	

1.1 Confidence Ranking

5 / 5

Very High Confidence

Guardian assigns a Confidence Ranking of 5 out of 5, combining finding severity, remediation outcome, and the reviewer’s assessment of latent risk. The full scale is on the next page.



1.2 Findings at a Glance

SEVERITY	TOTAL	PENDING	ACK	PARTIAL	RESOLVED
Critical	0	0	0	0	0
High	0	0	0	0	0
Medium	1	0	1	0	0
Low	4	0	3	0	1
Informational	2	0	0	0	2
All severities	7	0	4	0	3

§ 02

Confidence Ranking.

Guardian assigns a project-level confidence score using the scale below. The ranking combines finding severity, remediation outcome, and the reviewer's assessment of latent risk.

CONFIDENCE RANKING	DEFINITION AND RECOMMENDATION	RISK PROFILE
5 Very High Confidence ASSIGNED	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.	0 High/Critical findings and few Low/Medium severity findings.
4 High Confidence	Code is clean, well-structured, and adheres to best practices. Design patterns are sound and test coverage is strong. Recommendation: suitable for deployment after remediations; consider periodic review with changes.	0-1 High/Critical findings per engagement week and little to no Medium severity findings.
3 Moderate Confidence	Code is functional but shows gaps in defensive programming or test coverage. Recommendation: remediate the findings and re-review the changes before deployment.	Some High/Critical findings, with various Medium severity findings.
2 Low Confidence	Recurring issues suggest systemic gaps rather than isolated mistakes. Recommendation: remediate, then commission a follow-up review at a frozen commit.	Over 6 High and Critical findings across the engagement.
1 Very Low Confidence	The volume and severity of findings indicate the codebase is not ready for production. Recommendation: substantial rework, then a full re-review.	Over 12 High and Critical findings across the engagement.

§ 03

Scope & Classifications.

Guardian reviewed Conflux Deployment, USDT0 and CNHT0 in <https://github.com/everdawn-labs/usdt0-ofc-contracts>, <https://github.com/everdawn-labs/usdt0-tether-contracts-hardhat>.

IN SCOPE

- USDT0 OUpgradable: 0x2346d88699182f7c15cbfaa6e8824995eafab67a
- USDT0 OFT: 0xC57efa1c7113D98BdA6F9f249471704Ece5dd84A
- ProxyAdmin: 0xa882c21C9df00958A958cde96f2B2Ae8FB4315B1
- USDT0 Token: 0xaf37E8B6C9ED7f6318979f56Fc287d76c30847ff
- CHNT OFT (Conflux): 0x0200C29006150606B650577BBE7B6248F58470c1
- CHNT OFT Impl (Conflux): 0x5be536efB28c8EfbD2da6894996f5df88347d8B2
- CHNT OFT (Ethereum) : 0xA3CDdE086701839FbE255076d4730fF33F86C1cE
- CHNT OFT Impl (Ethereum): 0xcd62844E82cfEdf572B06275020254D40E016545
- CHNT Token (Conflux): 0xDed1660192d4d82e7c0B628ba556861EdBB5CAda
- CHNT Token Impl (Conflux): 0xedaba024be4d87974d5aB11C6Dd586963CcCB027
- RPC: <https://evm.confluxrpc.com>

3.1 Severity Matrix

	IMP · HIGH	IMP · MED	IMP · LOW
LIK · HIGH	Critical	High	Medium
LIK · MED	High	Medium	Low
LIK · LOW	Medium	Low	Low

IMPACT · HIGH	Significant loss of assets, harm to a group of users, or core protocol functionality is disrupted.
IMPACT · MEDIUM	Small amount of funds can be lost, or ancillary functionality is affected. Users may experience reduced or delayed receipt.
IMPACT · LOW	Unexpected behavior in some functionality that is notable but does not meet the criteria for higher severity.

§ 04

Findings.

Grouped by round. Visible IDs reset by severity within each round, so a finding is named the same way in the report as it was in the channel it was written in. Status is where each finding ended up; its own page says how.

ID	TITLE	CATEGORY	SEVERITY	STATUS	PAGE
MAIN REVIEW					
M-01	CHNT0 LZReceive Cannot Credit On Mainnet	—	MEDIUM	ACKNOWLEDGED	p. 7
L-01	Delegate Not Multi-Sig	—	LOW	RESOLVED	p. 8
L-02	Multiple Chains Not Connected To Conflux	—	LOW	ACKNOWLEDGED	p. 9
L-03	Duplicate Nonces On Safe	—	LOW	ACKNOWLEDGED	p. 10
I-01	Conflux Safe Has Different Signers	—	INFORMATIONAL	RESOLVED	p. 11
I-02	Peers/Configs Not Set	—	INFORMATIONAL	RESOLVED	p. 12
REMEDIATION REVIEW					
L-01	CNHT Token Does Not Support Zero Address	Warning	LOW	ACKNOWLEDGED	p. 13

MEDIUM **M-01**

ACKNOWLEDGED

CHNT0 LZReceive Cannot Credit On Mainnet

REVIEW

Main Review

— DESCRIPTION

The CHNT token on mainnet returns a `false` boolean value upon `transfer` since `StandardTokenWithFees.transfer` does not explicitly return a bool, defaulting to `false`:

```
```javascript
function transfer(address _to, uint _value) public returns (bool) {
 uint fee = calcFee(_value);
 uint sendAmount = _value.sub(fee);

 super.transfer(_to, sendAmount);
 if (fee > 0) {
 super.transfer(owner(), fee);
 }
}
```
```

Consequently, whenever an `LzReceive` message is received by the OFT on mainnet, any attempt to `transfer` will fail due to `SafeERC20` reverting with `SafeERC20FailedOperation`, as the `false` return is interpreted as a failed transfer.

— RECOMMENDATION

Adjust the `_credit` and `_debit` functions of the OFT Adapter on mainnet to avoid the `safeTransfer`.

— RESOLUTION

Status: Acknowledged.

LOW **L-01**

RESOLVED

Delegate Not Multi-Sig

LOCATION Global

REVIEW Main Review

DESCRIPTION

The delegate for CHNT0** **OFT `0x0200C29006150606B650577BBE7B6248F58470c1` ** **on Conflux is `0x1a6362AD64ccFF5902D46D875B36e8798267d154` which is not a multi-sig nor does it match the Safe address of `0x789498616f3Bb9F8dF52288A9311247028872105` .

RECOMMENDATION

Set the delegate to `0x789498616f3Bb9F8dF52288A9311247028872105`

RESOLUTION

Status: Resolved.

LOW **L-02**

ACKNOWLEDGED

Multiple Chains Not Connected To Conflux

REVIEW

Main Review

— DESCRIPTION

Chains Flare and Monad are not wired for the latest USDT0 deployment on Conflux.

— RECOMMENDATION

Ensure this is expected behavior.

— RESOLUTION

Status: Acknowledged.

LOW **L-03**

ACKNOWLEDGED

Duplicate Nonces On Safe

REVIEW

Main Review

— DESCRIPTION

Both Conflux and Mantle Safes have duplicate nonce 40, hence the second transaction to `setReceiveLibrary` will revert with `LZ_SameValue()`.

— RECOMMENDATION

Remove the duplicate tx.

— RESOLUTION

Status: Acknowledged.

INFORMATIONAL I-01

RESOLVED

Conflux Safe Has Different Signers

LOCATION Global
REVIEW Main Review

DESCRIPTION

Celo Safe has signers:

1. 0x4192D72c281dB0eF10464dD274EE583C33256ac5
2. 0x00F6D2b4B69Ce697f913Da16A9D73283dc4C78F2
3. 0x488A3d37442F583c1c0a356118d1d6181b22434c
4. 0x7D8e979dcC6EC933c70FBe28B2B7700907D2aFEA
5. 0x5F0DcA105195Bd58277aa4b4CABC90a791E1b982

But the Conflux Safe at 0x789498616f3Bb9F8dF52288A9311247028872105 has signers:

1. 0x1a6362AD64ccFF5902D46D875B36e8798267d154
2. 0x7D8e979dcC6EC933c70FBe28B2B7700907D2aFEA
3. 0x488A3d37442F583c1c0a356118d1d6181b22434c
4. 0x4192D72c281dB0eF10464dD274EE583C33256ac5
5. 0x5F0DcA105195Bd58277aa4b4CABC90a791E1b982

0x00F6D2b4B69Ce697f913Da16A9D73283dc4C78F2 is missing from the Conflux Safe and 0x1a6362AD64ccFF5902D46D875B36e8798267d154 was added.

RECOMMENDATION

Ensure the signers are intended on the Conflux Safe.

RESOLUTION

Status: Resolved.

INFORMATIONAL I-02

RESOLVED

Peers/Configs Not Set

LOCATION Global

REVIEW Main Review

— DESCRIPTION

Peers and configs are not currently set for Conflux and other chains, hence the existing block confirmations/DVN's/etc. do not currently match the intended configs.

— RECOMMENDATION

Ensure intended configs are set before cross-chain transfer is allowed.

— RESOLUTION

Status: Resolved.

LOW **L-01**

ACKNOWLEDGED

CNHT Token Does Not Support Zero Address

CATEGORY Warning

REVIEW Remediation Review

— DESCRIPTION

Unlike the USDT token, the CNHT token reverts on zero address transfer. Hence debited funds on src chain will not be credited on mainnet and the LayerZero message will be unfulfilled.

— RECOMMENDATION

Clearly document this behavior and consider crediting address(0) funds to the 0xdead address.

— RESOLUTION

Status: Acknowledged.

§ 05

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.

§ 06

About Guardian.

Guardian is a smart contract security firm. Every engagement is worked by two independent teams competing on the same scope, each with its own tooling and methods, so no single reviewer's blind spot survives.

\$45B+DIGITAL ASSETS UNDER
REVIEW**200+**

ENGAGEMENTS COMPLETED

500+CRITICAL & HIGH FINDINGS
REPORTED

Reach us at audits@guardianaudits.com.