15 Jul 2024

Zellic × Cytonic

Solana & EVM deposit contracts
Proposal

Executive Summary

Cytonic is seeking a security assessment of the Solana and EVM deposit contracts in its cytonic-bridge-solana and cytonic-bridge-evm repositories.

Zellic will perform an in-depth security assessment of the Solana and EVM deposit contracts in the cytonic-bridge-solana and cytonic-bridge-evm repositories. At a high level, we aim to detect and prevent protocol-breaking bugs that may lead to catastrophic consequences. Zellic approaches your application from a vulnerability research perspective, honed by our unique competitive hacking background and years of experience reviewing complex software. Our methodology is tailored specifically to your application and threat model. We consider multiple classes of security issues arising from, but not limited to, general coding mistakes, business logic issues, applied cryptographic errors, and design flaws. The review will also validate that the protocol implementation matches the desired specification.

Securing of the protocol will be performed during a single standalone audit. The primary security assessment will be performed over a 0.5 calendar-week period by 2 Zellic security engineers, for a total of 0.8 engineer-weeks. All remediations will also be verified by Zellic.

Introducing Zellic

Zellic is a security firm that has worked extensively with Layer 1s and leading protocols on EVM, Move (Aptos and Sui), and Solana, as well as Cairo, NEAR, and Cosmos. We identify complex vulnerabilities that threaten the future of blockchain projects.

Our background in traditional infosec and competitive hacking enables us to consistently discover hidden vulnerabilities and develop novel security research. Before Zellic, we founded the #1 CTF (competitive hacking) team in the world. It has earned us the reputation as the go-to security firm for teams whose rate of innovation outpaces the existing security landscape.

Among others, our clients include LayerZero, StarkWare, Mysten Labs, and Solana Foundation. We also have a strong internal team focused on rollups and ZK research, working on engagements with Scroll, Axiom, and Succinct Labs.

Zellic is backed by Sequoia Capital, Brevan Howard, Robot Ventures, and more. We are also a founding member of the Security Alliance (SEAL) led by samczsun, an industry effort to raise the bar for blockchain security.

Section 1. PROJECT BACKGROUND

Cytonic is the world's first Multi-Virtual-Machine Blockchain. The scope for review includes Cytonic bridge v1, which will be used to bootstrap liquidity for the Cytonic ecosystem. The bridge will eventually evolve to allow freely bridging assets between Cytonic and other blockchains.

Section 2. ZELLIC'S RELEVANT EXPERIENCE

Our auditors' training in cryptography, embedded systems, low-level exploitation, adversarial attacks, and traditional finance is particularly well suited for Cytonic's scope of work. We are uniquely positioned to integrate best practices from traditional infosec with the novelty and unique attack vectors of blockchain systems.

Zellic has earned a reputation as an expert in L1, L2, DeFi, and cross-chain security. We have successfully identified and remediated critical vulnerabilities across a wide range of engagements, many of which were missed by leading names in the industry. Some notable engagements relevant to Cytonic's scope are listed below. These outcomes are rooted in our fundamental approach to security and in the culture, processes, and leadership we have cultivated at Zellic.

Project	Description
Solana	L1 blockchain, Solana Mobile, and ecosystem primitives
Audius	Decentralized music streaming platform
Jump	Crypto division of Jump Trading Group
Eclipse	Parallelized L2 combining SVM, Celestia, Ethereum and RISC Zero technologies
Gravity Bridge	Decentralized Cosmos blockchain securing the operation of bridges between blockchains
Hyperliquid	Bridge deployed on Arbitrum
LayerZero	Omnichain interoperability protocol
Socket	Modular messaging bridge
StarGate	Fully composable omnichain liquidity transport protocol
Wormhole	Cross-chain messaging platform
Synapse	Cross-chain communications network
DefiVerse	NFT marketplace on the Oasys network
WorldInsight (eBridge)	First cross-chain bridge for aelf, permitting bidirectional transfers of the ELF token and Ethereum/BSC

Section 3. METHODOLOGY

During a security assessment, Zellic works through various testing methods along with a manual review. Alongside a variety of tools and analyzers used on an as-needed basis, we focus primarily on the following classes of security issues:

- **Basic coding mistakes:** Many critical vulnerabilities in the past have been caused by simple, surface-level mistakes that could have easily been caught ahead of time by code review. If possible, Zellic will analyze the scoped smart contract code using automated tools to detect these shallow bugs. Depending on the engagement, Zellic may also employ sophisticated analyzers such as model checkers, theorem provers, fuzzers, etc., as deemed necessary.

- **Business logic errors:** Business logic is the heart of any smart contract application. Zellic will manually review the contract logic to ensure that the code implements the expected functionality as specified in the Platform's design documents. If applicable, Zellic will also examine the specifications and designs themselves for inconsistencies, flaws, and vulnerabilities. This would involve use cases that open the opportunity for abuse, such as flawed tokenomics, share pricing, arbitrage opportunities, etc.

Apart from these, we will also look for issues pertaining to:

- **Test suite and code coverage:** We review the comprehensiveness of the project's test suite and code coverage. Untested code is error-prone and typically presents a security risk in general. On the other hand, certain testing practices like generative tests (like fuzzing), or property-based tests greatly improve the quality of a test suite and help mitigate security risks.

- **Libraries and frameworks:** Unsafe third-party libraries and frameworks can introduce security risks from beyond the project's first-party code. Hence, we review the de-pendencies, libraries, and frameworks used by the project.

Section 4. WORK EFFORTS

Work efforts have been determined based on a review of the scope as highlighted below in discussions with Cytonic.

Scope #1:

Source code location:
https://github.com/cytonic-network/cytonic-bridge-solana

Source code version:
Git commit 3553735e96ae29528870f1c0fc4c3354b80f8a63 in master

Files:

programs/depositor/*

Scope #2:

Source code location:
https://github.com/cytonic-network/cytonic-bridge-evm

Source code version:
Git commit 5a45f51b09f91444d01b0e1c23fd3b9016170702 in master

Files:
src/Depositor.sol

Excluding all test, mock, and interface files.

The assessment will require a total of 0.8 engineer-weeks over the course of a 0.5 calendar-week period by 2 Zellic security engineers.

Section 5. ESTIMATED PRICE & TIMELINE

Cytonic will pay the equivalent of $20,000 in USD or USDC stablecoin to provide a total of 0.8 engineer-weeks of availability. This payment is inclusive of all services defined in the proposal.

Section 6. DISCLAIMER

This proposed summary of terms is non-binding. No legally binding obligations will be created until definitive, signed agreements are delivered and executed in writing by both parties.