Review Summary of Bounties Network

Bug bounty Submission

OPENZEPPELIN SECURITY | DECEMBER 6, 2019

Security Audits

Bounties Network is a smart contract-based system for coordinating the creation of “bounties” for specific tasks, which are then paid out to individuals who volunteer to complete them. The Bounties Network serves individuals and communities globally, creating a new kind of mechanism to coordinate the incentivization of task completions.

Why we looked at it

Recently, Bounties Network introduced MetaTransaction support into their codebase. MetaTransactions solve several onboarding problems faced by Web3 applications. MetaTransactions abstract away the necessity of users to hold Ethereum in order to interact with smart contracts. Bounties Network chose to implement a custom MetaTransaction system design instead of choosing an open-source solution, such as the Gas Stations Network.

OpenZeppelin is a member of the Gas Stations Network Alliance and has audited the smart contracts that power the GSN Network. In addition to auditing the smart contracts (for which OpenZeppelin shared a grant from the Ethereum Foundation, along with TabooKey), the contracts were incorporated into the OpenZeppelin library of Audited smart contracts. OpenZeppelin has additionally created testing, production, and front-end tools to support projects looking to integrate meta-transactions into their codebase.

addition of issues in functions designed to add and replace approvers (one, two). Fortunately, the risk was minimal as the functions were not currently used in production. We responsibly disclosed our findings to Bounties Network and were awarded 1 ETH from Bounties Network’s Bug Bounty program. Bounties Network promptly addressed the issues, and they were corrected with the following commit.

While the errors we discovered were not critical, they do underscore the risks taken when building custom versions of infrastructure software. At OpenZeppelin, we believe that projects looking to implement functionality for which there already exist trusted solutions take on a higher level of risk and responsibility. We recommend, whenever possible, that projects rely on audited and battle-tested tools such as the smart contracts in the OpenZeppelin Smart Contract library. These tools are open source, audited, and continuously scrutinized by the community to ensure the highest level of security and safety available in the ecosystem today.

Related Posts

Beefy Zap Audit

BeefyZapRouter serves as a versatile intermediary designed to execute users' orders through routes...

Security Audits

OpenBrush Contracts Library Security Review

OpenBrush is an open-source smart contract library written in the Rust programming language and the...

Security Audits

Linea Bridge Audit

Linea is a ZK-rollup deployed on top of Ethereum. It is designed to be EVM-compatible and aims to...

Security Audits