External audit of OpenZeppelin

OPENZEPPELIN SECURITY | MAY 11, 2017

Security Audits

As you may know from reading our blog, we do lots of security audits for blockchain-based projects. All projects in the space need someone external to take a fresh, unbiased, and skeptic look at their code.

OpenZeppelin is an open repository of reusable smart contract modules. Since we started the project, we committed to the highest standard of security and peer-review. This means performing external audits on our code too. That's why we asked the New Alchemy team to perform a formal security audit of OpenZeppelin's codebase, following the 1.0.0 release of the framework.

Projects using OpenZeppelin just need to upgrade to the latest release (v1.0.5) to include the bugfixes coming from this audit. We're also working on a mechanism for on-chain upgradeability to enable already-deployed projects to receive security fixes.

The full audit can be found on GitHub, but this is a list of the most noteworthy findings and how we addressed them:

- Upgrade to latest Solidity version in all contracts. Fixed here.
- Prefer `throw` vs `return false`. This is in line with our fail early and loudly guideline. Fixed here.
- Create a cancellable pull payment helper class. Issue opened here.
- Create a version of PullPayment that checks the contract has enough balance to send. Issue opened here.

- ERC20 approve problem, as described in EDCON. Issue opened here.
- Create a simpler version of `MultisigWallet`. Issue opened here.

Most of the recommendations were implemented in this pull request. Other less urgent things were transformed into GitHub issues.

As always, we're committed to improving the security standards of the blockchain industry. This is a step forward in consolidating OpenZeppelin as a collection of reusable and secure modules anyone can use and extend.

If you're interested in discussing smart contract security, follow us on Medium, or apply to work with us! We're also available for smart contract security development and auditing work.

Related Posts

Beefy Zap Audit

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

OpenBrush Contracts Library Security Review

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

Security Audits

Security Audits