Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Audit-Results AERUM Smart Contract 09.2018

Cure53, Dr.-Ing. M. Heiderich, BSc. F. Fäßler

Audit Scope

- **AERUM Smart Contract**
  - https://github.com/AERUMTechnology/governance/blob/master/contracts/token/AerumToken.sol

Coverage

For the first round of the upcoming security audits, AERUM Technology provided Cure53 with the solidity code of the *AerumToken* contract. This contract is built upon the OpenZeppelin *Ownable* and *PausableToken* contracts. In the initially shared sources the precise OpenZeppelin version was not defined, but AERUM Technology provided these details promptly. Along the contract code, Cure53 also received documentation to verify that the token implements what AERUM Technology promises. This includes ensuring that the token is pausable, not mintable, not burnable and the initial supply is set correctly. Beyond verifying the claims, Cure53 also audited the technical security of the contract. This includes checking for typical ERC20 issues and general solidity pitfalls. Also AERUM Technology extended the OpenZeppelin base contracts and thus it had to be ensured, that this doesn't cause any security relevant side effects.

Results

The result of the first round of the security audit covering the *AerumToken* is very positive. Cure53 has verified that the *AerumToken* contract implements what AERUM Technology claims. All functions are pausable and tokens are not mintable and not burnable. It's also notable that AERUM Technology used recent contract versions from OpenZeppelin, which addressed a common race-condition issue regarding approvals, by implementing increase and decrease functions. The extension to the base contracts was implemented according to the best practices and no issues have been found. Overall the *AerumToken* contract is up to standard and deemed to be secure.

Final Words

Cure53 would like to thank Patrick O'Sullivan, Alex Randarevich and Petro Sidlovskyy from the AERUM Technology team for their excellent project coordination, support and assistance, both before and during this assignment.