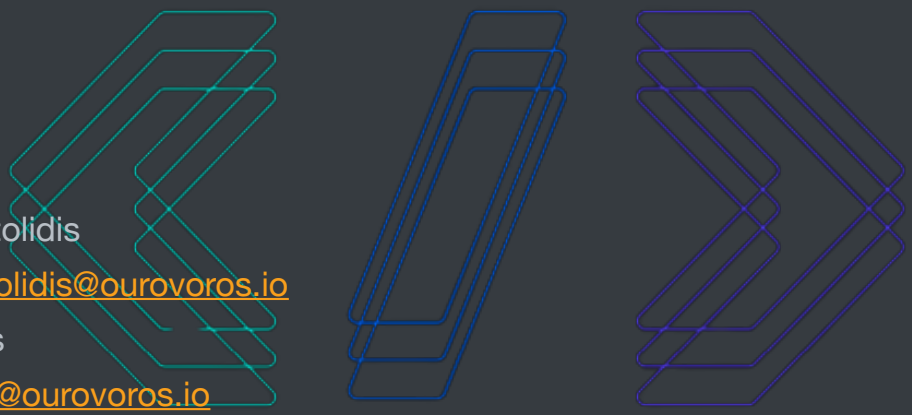
Immunefi

Vault Safe

Security Assessment & Correctness

May 2nd, 2023



Audited By:
Angelos Apostolidis
angelos.apostolidis@ourovoros.io
George Delkos
george.delkos@ourovoros.io

Overview

Project Summary

Project Name	Immunefi - Vault Safe
Website	Immunefi
Description	Bug Bounty Vaults
Platform	Ethereum; Solidity, Yul
Codebase	GitHub Repository
Commits	TBA

Audit Summary

Delivery Date	May 2nd, 2023
Method of Audit	Static Analysis, Manual Review

Vulnerability Summary

● **Total Issues**	0
● **Total Major**	0
● **Total Minor**	0
● **Total Informational**	0

Files In Scope

Contract	Location
src/Withdrawable.sol	TBA
src/Splitter.sol	TBA

Audit Notes

In this follow-up code audit, we have observed that the previously identified issues have been effectively addressed, enhancing the security and functionality of the codebase. The smart contracts have been updated to incorporate best practices, further improving their resilience against potential vulnerabilities.

During an internal due diligence process, the development team identified some areas for improvement, and the updated code successfully addresses these findings. The `Splitter` contract now offers a more secure and efficient way to process payments between security researchers and Immunefi.

Disclaimer

Reports made by Ourovoros are not to be considered as a recommendation or approval of any particular project or team. Security reviews made by Ourovoros for any project or team are not to be taken as a depiction of the value of the “product” or “asset” that is being reviewed.

Ourovoros reports are not to be considered as a guarantee of the bug-free nature of the technology analyzed and should not be used as an investment decision with any particular project. They represent an extensive auditing 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.

Each company and individual is responsible for their own due diligence and continuous security. Our goal is to help reduce the attack parameters and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claim any guarantee of security or functionality of the technology we agree to analyze.