



SMART CONTRACTS SECURITY AUDIT REPORTS



Audit Details



Audited Project

ArcadeFX



Deployer Address

[0x697Ac9951Ad8A1eb1a5a2cB5dc4225C236A9694d](#)



Client Contacts

ArcadeFX team



Blockchain

Binance Smart chain



Project website

www.arcadefx.games

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Coinvest and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Coinvest) owe no duty of care towards you or any other person, nor does Coinvest make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Coinvest hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Coinvest hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Coinvest, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

Coinvest was commissioned by ArcadeFX to perform an audit of smart contracts:

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified,

Avoiding Smart Contract Failures: The Benefits of Auditing

Contract failure: If a smart contract fails to perform as intended, it can result in significant financial losses. Auditing can help identify potential points of failure and ensure that contracts are robust and reliable.

Malicious attacks: Smart contracts can be targeted by hackers seeking to exploit weaknesses and steal funds. Auditing can help identify these vulnerabilities and implement appropriate security measures to prevent attacks.

Auditing smart contracts is essential to mitigate these risks and ensure that contracts perform as intended. With the increasing complexity of smart contracts and the growing importance of blockchain technology, auditing is more crucial than ever to ensure secure and reliable transactions.

Issues Checking Status

Issue description	Checking status
Compiler Errors	Passed
Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Malicious Event log	Passed
Economy model of the contract	Passed
Design Logic	Passed
Private user data leaks	Passed

The ArcadeFx smart contract is using secure openZeppelin templates, a standard in the blockchain industry.

Checking Functions

Issue description	Checking status
Compiler Errors	Passed
Owner Mint new tokens	No
Owner Contract Paused	No
ChangeOwner	Yes
Burn function	No
RenounceOwner	No
Connect external contracts	No

Contract Creator: [0x59da13a12a09da0bbd5a2dcec84750334a4abf6f](#)

Security Issues



High Severity Issues

No high severity issues found.



Medium Severity Issues

No medium severity issues found.



Low Severity Issues

No low severity issues found.

Smart contracts do not contain high severity issues!

Coinvest note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts **deployed by Owner**