ARBICHECK

Exxpad

Smart Contract Audit

🌐 arbicheck.com

📲 arbicheck

Table of Contents

Audit Summary

Project Name	Exxpad
Contract Address	0x5f6061203D515141eCa5A2fA98ea6Da6649bfCCd
Deployer Address	0x3187d7b392f74388f5dd17525beff8a6f7bcb11e
Website	https://exxpad.com/
Language	Solidity
Blockchain	Arbitrum
Audit Date	June 02 2023

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.

This audit report has been prepared by Arbicheck's experts at the request of the client. 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.

Audit Scope

Arbicheck team was commissioned by Exxpad to perform an audit based on the following smart contracts:

https://arbiscan.io/address/0x5f6061203d515141eca5a2fa98ea6da6649bfccd#code

Note that we **ONLY** audited the code available to us on this URL at the time of the audit. If the URL is not from any block explorer (main net), it may be subject to change. Always check the contract address on this audit report and compare it to the token you are doing research for.

SWC Attack Analysis

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in [EIP-1470](#).

ID	Description	Status
SWC-100	Function Default Visibility	Not Found
SWC-101	Integer Overflow and Underflow	Not Found
SWC-102	Outdated Compiler Version	Not Found
SWC-103	Floating Pragma	Not Found
SWC-104	Unchecked Call Return Value	Not Found
SWC-105	Unprotected Ether Withdrawal	Not Found
SWC-106	Unprotected SELF DESTRUCT Instruction	Not Found
SWC-107	Reentrancy	Not Found
SWC-108	State Variable Default Visibility	Not Found
SWC-109	Uninitialized Storage Pointer	Not Found
SWC-110	Assert Violation	Not Found
SWC-111	Use of Deprecated Solidity Functions	Not Found
SWC-112	Delegatecall to Untrusted Callee	Not Found
SWC-113	DoS with Failed Call	Not Found
SWC-114	Transaction Order Dependence	Not Found
SWC-115	Authorization through tx.origin	Not Found
SWC-116	Block values as a proxy for time	Not Found

SWC-117	Signature Malleability	Not Found
SWC-118	Incorrect Constructor Name	Not Found
SWC-119	Shadowing State Variables	Not Found
SWC-120	Weak Sources of Randomness from Chain Attributes	Not Found
SWC-121	Missing Protection against Signature Replay Attacks	Not Found
SWC-122	Lack of Proper Signature Verification	Not Found
SWC-123	Requirement Violation	Not Found
SWC-124	Write to Arbitrary Storage Location	Not Found
SWC-125	Incorrect Inheritance Order	Not Found
SWC-126	Insufficient Gas Grieng	Not Found
SWC-127	Arbitrary Jump with Function Type Variable	Not Found
SWC-128	DoS With Block Gas Limit	Not Found
SWC-129	Typographical Error	Not Found
SWC-130	Right-To-Left-Override control character (U+202E)	Not Found
SWC-131	Presence of unused variables	Not Found
SWC-132	Unexpected Ether balance	Not Found
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Not Found
SWC-134	Message call with hardcoded gas amount	Not Found
SWC-135	Code With No Effects	Not Found
SWC-136	Unencrypted Private Data On-Chain	Not Found

Slither Analysis

Impact	Confidence	Description
Informational	Medium	ERC20._burn(address,uint256) (a.sol#419-435) is never used and should be removed
Informational	Medium	Context._msgData() (a.sol#26-28) is never used and should be removed
Informational	Medium	ExxPad.constructor() (a.sol#517-519) uses literals with too many digits: - _mint(msg.sender,10000000 * 10 ** decimals()) (a.sol#518)

Owner Privileges

- No owner privileges found

Risk Classification

Arbicheck uses certain vulnerability levels, these indicate how bad a certain issue is. The higher the risk, the more strictly it is recommended to correct the error before using the contract.

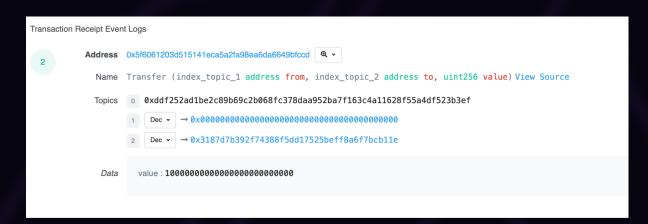| Vulnerability Level	Description
High Issues	These issues will cause the problems and SHOULD be adjusted
Medium Issues	These issues will likely cause the problems and recommended to be adjusted
Low Issues	These issues will not cause any problems, but can be adjusted for the improvement
Notes	Does not compromise the functionality of the contract and just the general recommendations

Not used function

Notes

Recommendation

_burn function has no usage and could be removed from contract.

Deploy Snapshot

⑦ Transaction Hash:	0x28cc90c6fa7a1cd1a9248a2ded7c04774b991145bc202c19c628a30a81cc49b4 ⧉
⑦ Status:	✓ Success
⑦ Block:	96691012 ⟩ 34532 L1 Block Confirmations
⑦ Timestamp:	⏱ 4 days 20 hrs ago (Jun-01-2023 01:04:40 PM +UTC)
⑦ From:	0x3187d7b392f74388f5dd17525beff8a6f7bcb11e ⧉
⑦ Interacted With (To):	[Contract 0x5f6061203d515141eca5a2fa98ea6da6649bfccd Created] ✓ ⧉
⑦ ERC-20 Tokens Transferred:	▸ From Null: 0x000…… To 0x3187d7b392f74… For 10,000,000 ◎ ExxPad (XPAD)
⑦ Value:	0 ETH ($0.00)
⑦ Transaction Fee:	0.0007689292 ETH ($1.40)
⑦ Gas Price Bid:	0.0000000026 ETH (2.6 Gwei)
⑦ Gas Price Paid:	0.0000000001 ETH (0.1 Gwei)
⑦ Ether Price:	$1,862.13 / ETH
⑦ Gas Limit & Usage by Txn:	8,562,461	7,689,292 (89.8%)

Transaction Receipt Event Logs

Address 0x5f6061203d515141eca5a2fa98ea6da6649bfccd 🔍⌄

Name Transfer (index_topic_1 address from, index_topic_2 address to, uint256 value) View Source

Topics 0 0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef

1 Dec⌄ → 0x0000000000000000000000000000000000000000

2 Dec⌄ → 0x3187d7b392f74388f5dd17525beff8a6f7bcb11e

Data value : 10000000000000000000000000

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice 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 disclaimer below – please make sure to read it in full.

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 Arbicheck and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (Arbicheck) owe no duty of care towards you or any other person, nor does Arbicheck 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 Arbicheck 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, Arbicheck hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Arbicheck, 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 the 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. Arbicheck owns all copyright rights to the text, images, photographs, and other content provided in the following document. When using or sharing partly or in full, third parties must provide a direct link to the original document mentioning the author (arbicheck.com).