



SMART CONTRACT SECURITY AUDIT OF



Ice Bear Society

Summary

Audit Firm: Guardian Audits

Client Firm: Ice Bear Society


Final Report Date - Preliminary Report

Audit Summary

After a line by line manual analysis and automated review, Guardian Audits has concluded that:

- Ice Bear Society's smart contracts have a **LOW RISK SEVERITY**
- Ice Bear Society's smart contracts have an **ACTIVE OWNERSHIP**
- Important owner privileges – `reserveForGiveaway`, `setSaleTime`, `setCost`, `setMaxMintAmount`, `setBaseURI`, `pause`, `withdraw`
- Ice Bear Society's smart contract owner has multiple "write" privileges. Centralization risk correlated to the active ownership is **MEDIUM**

Notice that the examined smart contracts are not resistant to internal exploit. For a detailed understanding of risk severity, source code vulnerability, and potential attack vectors, refer to the complete audit report below.

 Ice Bear Society's contract address: **0xF33925C8F4C13ae138C8E7D159e950824990eA36**

 Blockchain network: **Fantom Opera**

 Verify the authenticity of this report on Guardian's GitHub: <https://github.com/guardianaudits>


 Comprehensive code coverage + fuzzing test suite:
https://github.com/GuardianAudits/IceBearSociety_TestSuite

Table of Contents

Project Information

Overview 4

Audit Scope & Methodology 5

Smart Contract Risk Assessment

Inheritance Graph 6

Findings & Resolutions 7

Report Summary

Auditor’s Verdict 13

Addendum

Disclaimer 14

About Guardian Audits 15

Project Overview

Project Summary

Project Name	Ice Bear Society
Language	Solidity
Codebase	https://ftmscan.com/address/0xF33925C8F4C13ae138C8E7D159e950824990eA36
Commit	N/A

Audit Summary

Delivery Date	Preliminary Report
Audit Methodology	Static Analysis, Manual Review, Full Test Suite, Fuzzing

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
● Critical	0	0	0	0	0	0
● High	0	0	0	0	0	0
● Medium	2	2	0	0	0	0
● Low	3	3	0	0	0	0

Audit Scope & Methodology

Scope

ID	File	SHA-1 Checksum
ICE	IceBearSociety.sol	2079BD4DE127DFE9D5A56A7811927054711D0BF6

Methodology

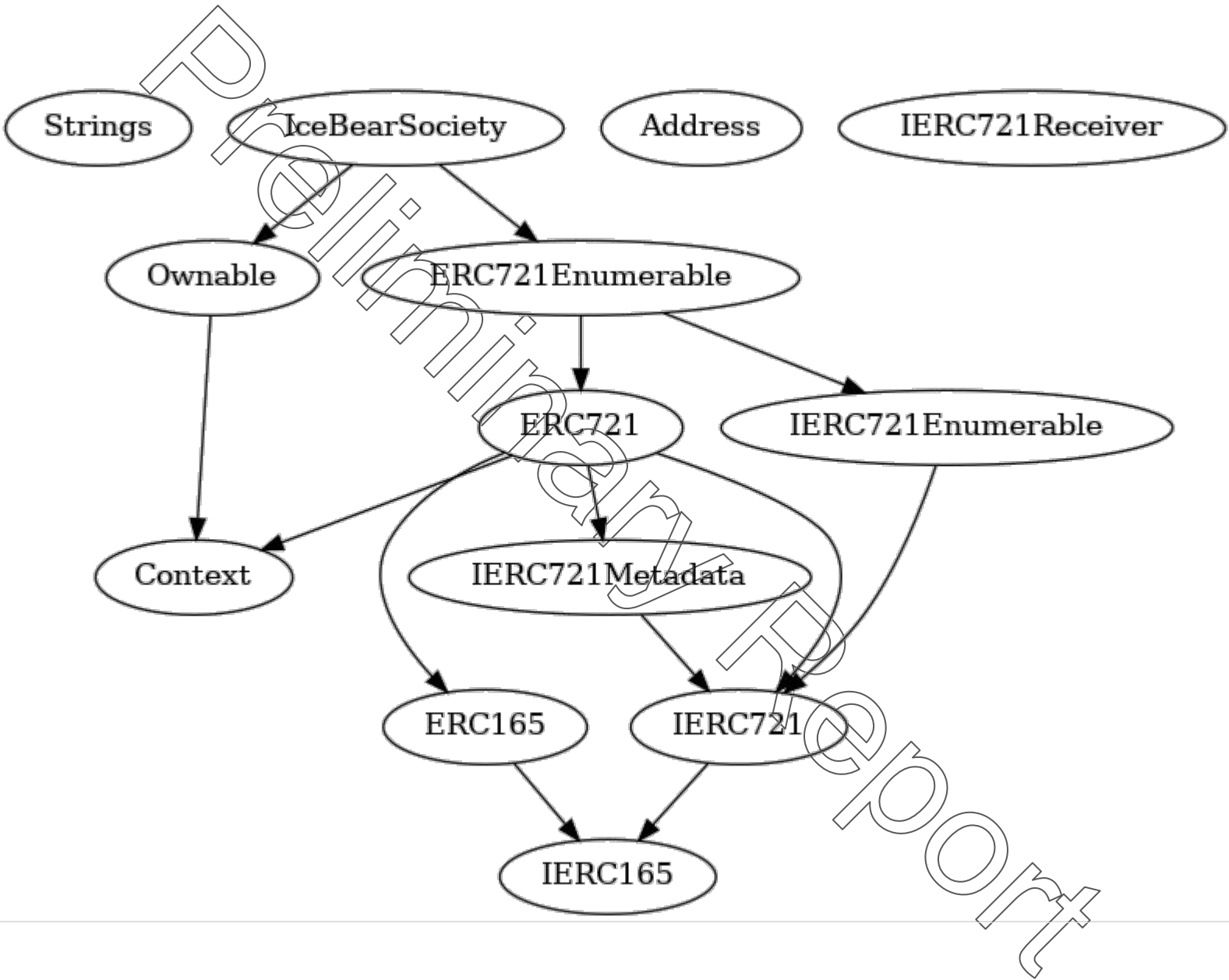
The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.
- Comprehensive written tests as a part of a 100% code coverage testing suite.
- **Premium:** Contract fuzzing for increased attack resilience

Vulnerability Classifications

Vulnerability Level	Classification
● Critical	Easily exploitable by anyone, causing loss/manipulation of assets or data.
● High	Arduously exploitable by a subset of addresses, causing loss/manipulation of assets or data.
● Medium	Inherent risk of future exploits that may or may not impact the smart contract execution.
● Low	Minor deviation from best practices.

Inheritance Graph



Findings & Resolutions

ID	Title	Category	Severity	Status
<u>ICE-1</u>	Centralization Risk	Centralization / Privilege	● Medium	Unresolved
<u>ICE-2</u>	Uncapped Minting	Logical Error	● Medium	Unresolved
<u>ICE-3</u>	Immutability Modifiers	Mutability	● Low	Unresolved
<u>ICE-4</u>	Function Visibility Modifiers	Optimization	● Low	Unresolved
<u>ICE-5</u>	Block Timestamp	Tx Manipulation	● Low	Unresolved

ICE-1 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	● Medium	IceBearSociety.sol	Unresolved

Description

The owner address, 0xa3056090d5583747ef278f3cb6d599aa0e306e64, is not a multi-sig and has potentially dangerous permissions for renounceOwnership, transferOwnership, reserveForGiveaway, setSaleTime, setCost, setMaxMintAmount, setBaseURI, pause, withdraw, and a modified mint execution where the owner can mint Ice Bear NFTs for free.

Recommendation

Make the owner a multi-sig and/or introduce a timelock for improved community oversight.

Resolution

ICE-2 | Uncapped Minting

Category	Severity	Location	Status
Logical Error	● Medium	IceBearSociety.sol:1286	Unresolved

Description

The owner can cause the `totalSupply` to exceed the `maxSupply` by calling `reserveForGiveaway` with an arbitrarily large amount.

Recommendation

Add a `require` or an `if` statement to make sure the amount of tokens to reserve plus the current supply does not exceed the max supply.

Resolution

ICE-3 | Immutability Modifiers

Category	Severity	Location	Status
Mutability	● Low	IceBearSociety.sol:1268	Unresolved

Description

The devAddress, maxSupply, and baseExtension variables are never modified, and should therefore be declared constant.

Recommendation

Declare them as constant.

Resolution

ICE-4 | Function Visibility Modifiers

Category	Severity	Location	Status
Optimization	● Low	IceBearSociety.sol	Unresolved

Description

The functions `mint`, `walletOfOwner`, `setCost`, `setMaxMintAmount`, `setBaseURI`, `pause`, and `withdraw` are marked as `public`, but are never called from inside the contract.

Recommendation

These functions can be marked `external` for gas optimization and explicitness.

Resolution

ICE-5 | Block Timestamp

Category	Severity	Location	Status
Tx Manipulation	● Low	IceBearSociety.sol	Unresolved

Description

The mint function relies on block.timestamp which can be manipulated by validators in extreme circumstances.

Recommendation

The block.timestamp reliance can be safely ignored as the saleStart takes place in the past.

While block.timestamp may be more accurate for auction time, it can be manipulated by validators. In the future, it may help to rely on block.number instead, or ensure resilience to block.timestamp manipulation.

Resolution

Auditor's Verdict

After a line by line manual analysis and automated review, Guardian Audits has concluded that:

- Ice Bear Society's smart contracts have a **LOW RISK SEVERITY**
- Ice Bear Society's smart contracts have an **ACTIVE OWNERSHIP**
- Important owner privileges – `reserveForGiveaway`, `setSaleTime`, `setCost`, `setMaxMintAmount`, `setBaseURI`, `pause`, `withdraw`
- Ice Bear Society's smart contract owner has multiple "write" privileges. Centralization risk correlated to the active ownership is **MEDIUM**

Disclaimer

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Guardian to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Guardian’s position is that each company and individual are responsible for their own due diligence and continuous security. Guardian’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by Guardian is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

Notice that smart contracts deployed on the blockchain are not resistant from internal/external exploit. Notice that active smart contract owner privileges constitute an elevated impact to any smart contract’s safety and security. Therefore, Guardian does not guarantee the explicit security of the audited smart contract, regardless of the verdict.

About Guardian Audits

Founded in 2022 by DeFi experts, Guardian Audits is a leading audit firm in the DeFi smart contract space. With every audit report, Guardian Audits upholds best-in-class security while achieving our mission to relentlessly secure DeFi.

To learn more, visit <https://guardianaudits.com>

To view our audit portfolio, visit <https://github.com/guardianaudits>

To book an audit, message <https://t.me/guardianaudits>