AstraSec

INTOS Token
Security Audit Report

January 27, 2025

Contents

1 Introduction

1.1 About INTOS Token

INT OS is built on WEBisOpen's advanced architectural infrastructure, designed to seamlessly transform AI agents from theoretical research concepts into practical, real-world applications. The audited INTOS token functions as the governance token, driving and empowering the INT OS platform.

1.2 Source Code

The following source code was reviewed during the audit:

- https://basescan.org/address/0x42e07fA3d31190731368Ca2F88D12D80139DCa42#code

2 Overall Assessment

This report has been compiled to identify issues and vulnerabilities within the INTOS token. Throughout this audit, we conducted a comprehensive analysis of the token contract's design and implementation. This included a manual review of the business logic, an examination of system operations, and a detailed evaluation of ERC20-related components to identify any potential flaws or inconsistencies.

Additionally, we thoroughly assessed the contract's adherence to the standard ERC20 specification, evaluated its alignment with industry best practices, and validated its compatibility with other ERC20 tokens and current DeFi protocols. The findings of our ERC20 compliance checks are detailed in Section 3.

Overall, no vulnerabilities or ERC20 compliance issue was found and our detailed checklist can be found in Section 3.

Severity	Count	Acknowledged	Won't Do	Addressed
Critical	–	–	–	–
High	–	–	–	–
Medium	–	–	–	–
Low	–	–	–	–
Informational	–	–	–	–
Undetermined	–	–	–	–

3 ERC20 Compliance Checks

3.1 ERC20 Token Methods

ERC20 is a standard for fungible tokens, ensuring compatibility and interoperability with platforms, wallets, and exchanges. This section reviews the INTOS token's implementation by examining its ERC20 methods and events, validating compliance with the ERC20 specification.

Method	Specification	Status
name	Returns the name of the token as a string. e.g., “MyToken“	✔
symbol	Returns the symbol of the token. e.g., “HIX”	✔
decimals	Returns the number of decimals the token uses. e.g., 18	✔
totalSupply	Returns the total token supply	✔
balanceOf	Returns the account balance of any address	✔
transfer	Returns a boolean value reflecting the token transfer status	✔
	Throws if the caller does not have enough balance	✔
	Transfers of 0 values must be treated as normal transfers	✔
	Fires the Transfer event	✔
transferFrom	Returns a boolean value reflecting the token transfer status	✔
	Throws if the spender does not have enough token allowances	✔
	Throws if the from address does not have enough balance	✔
	Transfers of 0 values must be treated as normal transfers	✔
	Fires the Transfer event	✔
approve	Returns a boolean value reflecting the token approval status	✔
	Fires the Approval event	✔
allowance	Returns the amount which the spender is still allowed to withdraw from the owner	✔

3.2 ERC20 Events

Event	Specification	Status
Transfer	MUST trigger when tokens are transferred, including zero value transfers	✔
	SHOULD trigger with the from address set to $0x0$ when tokens are created	✔
Approval	MUST trigger on any successful call to approve()	✔

The tables above present the checklists for ERC20 methods and events, evaluated against the ERC20 token standard. Our analysis confirms that the INTOS Token fully implements all required methods and events in compliance with the ERC20 specification. No inconsistencies or incompatibilities with the ERC20 standard were identified during the review.

4 Vulnerability Summary

4.1 Overview

After completing the audit, we conclude that the implementation of the INTOS token is well-structured and expertly engineered, with no vulnerability identified.

4.2 Security Level Reference

In web3 smart contract audits, vulnerabilities are typically classified into different severity levels based on the potential impact they can have on the security and functionality of the contract. Here are the definitions for critical-severity, high-severity, medium-severity, and low-severity vulnerabilities:

Severity	Acknowledged
C-X (Critical)	A severe security flaw with immediate and significant negative consequences. It poses high risks, such as unauthorized access, financial losses, or complete disruption of functionality. Requires immediate attention and remediation.
H-X (High)	Significant security issues that can lead to substantial risks. Although not as severe as critical vulnerabilities, they can still result in unauthorized access, manipulation of contract state, or financial losses. Prompt remediation is necessary.
M-X (Medium)	Moderately impactful security weaknesses that require attention and re-mediation. They may lead to limited unauthorized access, minor financial losses, or potential disruptions to functionality.
L-X (Low)	Minor security issues with limited impact. While they may not pose significant risks, it is still recommended to address them to maintain a robust and secure smart contract.
I-X (Informational)	Warnings and things to keep in mind when operating the protocol. No immediate action required.
U-X (Undetermined)	Identified security flaw requiring further investigation. Severity and impact need to be determined. Additional assessment and analysis are necessary.

5 Appendix

5.1 About AstraSec

AstraSec is a blockchain security company that serves to provide high-quality auditing services for blockchain-based protocols. With a team of blockchain specialists, AstraSec maintains a strong commitment to excellence and client satisfaction. The audit team members have extensive audit experience for various famous DeFi projects. AstraSec's comprehensive approach and deep blockchain understanding make it a trusted partner for the clients.

5.2 Disclaimer

The information provided in this audit report is for reference only and does not constitute any legal, financial, or investment advice. Any views, suggestions, or conclusions in the audit report are based on the limited information and conditions obtained during the audit process and may be subject to unknown risks and uncertainties. While we make every effort to ensure the accuracy and completeness of the audit report, we are not responsible for any errors or omissions in the report.

We recommend users to carefully consider the information in the audit report based on their own independent judgment and professional advice before making any decisions. We are not responsible for the consequences of the use of the audit report, including but not limited to any losses or damages resulting from reliance on the audit report.

This audit report is for reference only and should not be considered a substitute for legal documents or contracts.

5.3 Contact

Phone	+86 156 0639 2692
Email	contact@astrasec.ai
Twitter	https://twitter.com/AstraSecAI