BAIL security

BAILSEC.IO

EMAIL : OFFICE@BAILSEC.IO

TWITTER : @BAILSECURITY

TELEGRAM : @HELLOATBAILSEC

FINAL REPORT:

CVE Token

October 2023

Disclaimer:

Security assessment projects are time-boxed and often reliant on information that may be provided by a client, its affiliates, or its partners. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

The content of this assessment is not an investment. The information provided in this report is for general informational purposes only and is not intended as investment, legal, financial, regulatory, or tax advice. The report is based on a limited review of the materials and documentation provided at the time of the audit, and the audit results may not be complete or identify all possible vulnerabilities or issues. The audit is provided on an "as-is," "where-is," and "as-available" basis, and the use of blockchain technology is subject to unknown risks and flaws.

The audit does not constitute an endorsement of any particular project or team, and we make no warranties, expressed or implied, regarding the accuracy, reliability, completeness, or availability of the report, its content, or any associated services or products. We disclaim all warranties, including the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

We assume no responsibility for any product or service advertised or offered by a third party through the report, any open-source or third-party software, code, libraries, materials, or information linked to, called by, referenced by, or accessible through the report, its content, and the related services and products. We will not be liable for any loss or damages incurred as a result of the use or reliance on the audit report or the smart contract.

The contract owner is responsible for making their own decisions based on the audit report and should seek additional professional advice if needed. The audit firm or individual assumes no liability for any loss or damages incurred as a result of the use or reliance on the audit report or the smart contract. The contract owner agrees to indemnify and hold harmless the audit firm or individual from any and all claims, damages, expenses, or liabilities arising from the use or reliance on the audit report or the smart contract.

By engaging in a smart contract audit, the contract owner acknowledges and agrees to the terms of this disclaimer.

1. Project Details

Project	CVE Token
Website	N/A
Type	Token
Language	Solidity
Methods	Manual Analysis
Github repository	https://github.com/Chainverge/SmartContracts/blob/ae750be9203ab23b6c7ddcb11c1c0001181e8fb5/CVE%20Token

2. Detections Overview

Severity	Found	Resolved	Partially Resolved	Acknowledged (no change made)
High	0			
Medium	0			
Low	0			
Informational	1			
Governance	1			
Quality assurance	0			
Total	2			

2.1 Detections Definitions

Severity	Description
High	The problem poses a significant threat to the confidentiality of a considerable number of users' sensitive data. It also has the potential to cause severe damage to the client's reputation or result in substantial financial losses for both the client and the affected users.
Medium	While medium level vulnerabilities may not be easy to exploit, they can still have a major impact on the execution of a smart contract. For instance, they may allow public access to critical functions, which could lead to serious consequences.
Low	Poses a very low-level risk to the project or users. Nevertheless the issue should be fixed immediately
Informational	Effects are small and do not post an immediate danger to the project or users
Governance	Governance privileges which can directly result in a loss of funds or other potential undesired behavior
Qauality assurance	Aggregated minor issues, ensuring a high quality codebase.

3. Detections

BurnableTaxToken

The `BurnableTaxToken` is an ERC20 token that integrates functionalities from OpenZeppelin's esteemed ERC20Burnable library, ensuring a foundation of tested and trusted code. This token introduces a distinct transfer-tax mechanism. On every transfer, to or from an AMM pair, which indicates a buy or sell transaction, a fee of up to 1% can be levied, part of which is burned, permanently removing it from circulation, and the rest is directed to a designated fee address. This fee structure supports both deflationary and revenue-generating mechanics, contingent on the ratio set between burning and fee distribution. To cater to strategic partnerships or privileged users, the token introduces a whitelisting mechanism. If either the sender or recipient of a transfer is whitelisted, the transaction is exempted from the fee, facilitating tax-free transfers. This offers a level of flexibility to encourage specific transactions or partnerships. The initial supply of the token is minted by the owner during contract deployment. This supply is capped, meaning the owner cannot mint beyond this initial issuance, ensuring predictability in the token's monetary policy. Additionally, while the fee address, which receives part of the transfer tax, is mutable, any changes made to it will be transparent, ensuring that the community is informed of any revenue redirection. Overall, this token melds tried-and-true functionalities with innovative features, striking a balance between usability, revenue generation, and deflationary characteristics. Proper governance and communication channels will be key to leveraging these functionalities for the benefit of all stakeholders.

Issue	Adjustable fee and whitelist mechanism
Severity	Governance
Description	The ERC20 TaxToken's whitelist feature introduces potential centralization issues, as the owner possesses the power to grant certain addresses tax-free transactions. This preferential treatment may result in uneven economic dynamics within the token ecosystem. Moreover, large whitelisted token holders can significantly influence tokenomics by conducting vast tax-exempt transfers. Without transparent governance, this structure could lead to market manipulations and erode trust among regular token holders.
Recommendations	We highly recommend informing the community before such changes.
Comments / Resolution	

Issue	Lack of events
Severity	Informational
Description	Certain functionalities are changing sensitive state variables, however, these do not emit corresponding events.
Recommendations	We recommend implementing events for whitelisting and fee adjustment.
Comments / Resolution	