ETHGas

ERC20 Token

Security Assessment Report

Version: 2.0

January, 2026

Contents

Introduction

Sigma Prime was commercially engaged to perform a time-boxed security review of the ETHGas components in scope. The review focused solely on the security aspects of the Solidity implementation of the contract, though general recommendations and informational comments are also provided.

Disclaimer

Sigma Prime makes all effort but holds no responsibility for the findings of this security review. Sigma Prime does not provide any guarantees relating to the function of the components in scope. Sigma Prime makes no judgements on, or provides any security review, regarding the underlying business model or the individuals involved in the project.

Document Structure

The first section provides an overview of the functionality of the ETHGas components contained within the scope of the security review. A summary followed by a detailed review of the discovered vulnerabilities is then given which assigns each vulnerability a severity rating (see Vulnerability Severity Classification), an *open/closed/resolved* status and a recommendation. Additionally, findings which do not have direct security implications (but are potentially of interest) are marked as *informational*.

The appendix provides additional documentation, including the severity matrix used to classify vulnerabilities within the ETHGas components in scope.

Overview

The ETHGas ERC20 token contract is a standard ERC20 token contract that is used to represent the ETHGas token.

Security Assessment Summary

Scope

The review was conducted on the files hosted on the ethgas-developer/ethgas-contracts-core-new-for-audit repository.

The scope of this time-boxed review was strictly limited to `EthgasToken.sol` at commit 0718b21.

The token is deployed at address: 0x2798b1cc5a993085e8a9d46e80499f1b63f42204.

Note: third party libraries and dependencies were excluded from the scope of this assessment.

Approach

The security assessment covered components written in Solidity.

For the Solidity components, the manual review focused on identifying issues associated with the business logic implementation of the contracts. This includes their internal interactions, intended functionality and correct implementation with respect to the underlying functionality of the Ethereum Virtual Machine (for example, verifying correct storage/memory layout).

Additionally, the manual review process focused on identifying vulnerabilities related to known Solidity anti-patterns and attack vectors, such as re-entrancy, front-running, integer overflow/underflow and correct visibility specifiers.

To support the Solidity components of the review, the testing team may use the following automated testing tools:

- Aderyn: `https://github.com/Cyfrin/aderyn`
- Slither: `https://github.com/trailofbits/slither`
- Mythril: `https://github.com/ConsenSys/mythril`

Output for these automated tools is available upon request.

Coverage Limitations

Due to the time-boxed nature of this review, all documented vulnerabilities reflect best effort within the allotted, limited engagement time. As such, Sigma Prime recommends to further investigate areas of the code, and any related functionality, where majority of critical and high risk vulnerabilities were identified.

Findings Summary

The testing team identified a total of 1 issues during this assessment. Categorised by their severity:

- Informational: 1 issue.

Detailed Findings

This section provides a detailed description of the vulnerabilities identified within the ETHGas components in scope. Each vulnerability has a severity classification which is determined from the likelihood and impact of each issue by the matrix given in the Appendix: Vulnerability Severity Classification.

A number of additional properties of the components, including optimisations, are also described in this section and are labelled as “informational”.

Each vulnerability is also assigned a **status**:

- ***Open:*** the issue has not been addressed by the project team.
- ***Resolved:*** the issue was acknowledged by the project team and updates to the affected components(s) have been made to mitigate the related risk.
- ***Closed:*** the issue was acknowledged by the project team but no further actions have been taken.

Summary of Findings

ID	Description	Severity	Status
EGT-01	Solidity Compiler Version	Informational	**Closed**

EGT-01	Solidity Compiler Version
Asset	`EthgasToken.sol`
Status	**Closed:** See Resolution
Rating	Informational

Description

The token contract is using the solidity compiler version `^0.8.20`, which is a floating version.

This is different compared to the version used in `EthgasPool.sol` which is `^0.8.28`.

Recommendations

Consider using a consistent fixed version for all contracts.

Resolution

The development team has acknowledged this issue.

Appendix A Vulnerability Severity Classification

This security review classifies vulnerabilities based on their potential impact and likelihood of occurance. The total severity of a vulnerability is derived from these two metrics based on the following matrix.

		Likelihood		
		Low	Medium	High
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Low	Low	Medium

Table 1: Severity Matrix - How the severity of a vulnerability is given based on the *impact* and the *likelihood* of a vulnerability.