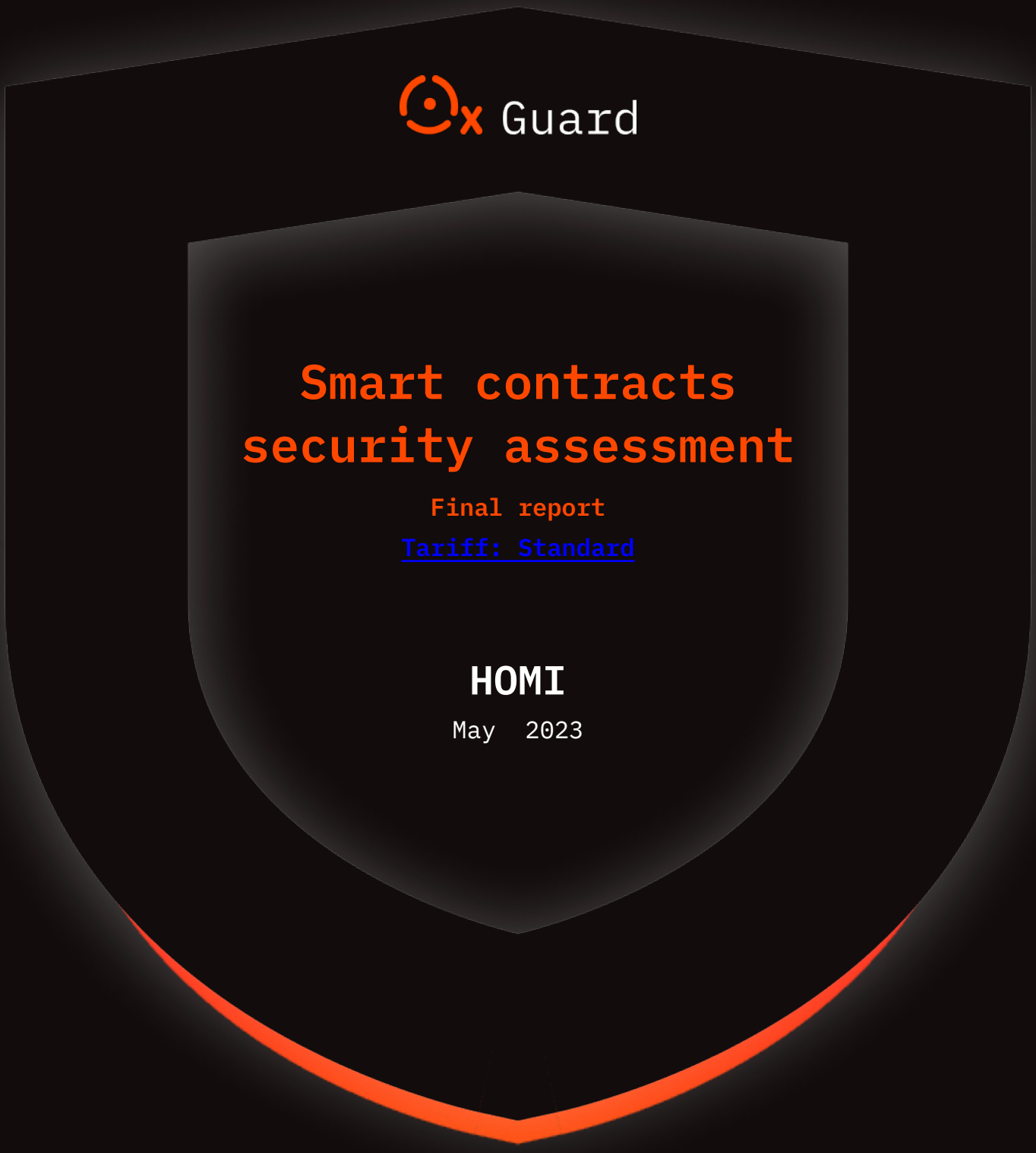

Guard

Smart contracts security assessment

Final report

Tariff: Standard

HOMI

May 2023

0xguard.com

hello@0xguard.com

Contents

1. Introduction 3
2. Contracts checked 3
3. Procedure 3
4. Classification of issue severity 4
5. Issues 4
6. Conclusion 5
7. Disclaimer 6

Introduction

The report has been prepared for **HOMI**.

The HOMI contract is a fungible token with the owner that has the capability to mint and burn tokens of any user.

22000000 tokens are preminted to the owner address in the contract constructor.

The md5 sum of the file under investigation:

33c3c69274b5330157e5a9f58359c1b6 - homi.move

Name	HOMI
Audit date	2023-05-22 - 2023-05-26
Language	Move
Platform	Sui

Contracts checked

Name	Address
Homi	

Procedure

We perform our audit according to the following procedure:

Manual audit

- Manually analyze smart contracts for security vulnerabilities
- Smart contracts' logic check

Classification of issue severity

High severity	High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.
Medium severity	Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.
Low severity	Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

No issues were found

Medium severity issues

No issues were found

Low severity issues

1. Invalid comment (Homi)

Status: Open

Consider replacing '`MANAGED`' with '`HOMI`' in the description on L15.

Conclusion

HOMI Homi contract was audited. 1 low severity issue was found.

The contract owner can mint or burn tokens of any user. Thus, users interacting with the contract must trust the owner.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without 0xGuard prior written consent.

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 0xGuard 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.
OxGuard retains exclusive publishing rights for the results of this audit on its website and social networks.

0x Guard