// Private Smart Contract Security Assessment 04.22.2024 - 05.17.2024

Amber
Trust Wallet

HALBORN

Amber - Trust Wallet

Prepared by: HALBORN

Last Updated 06/03/2024

Date of Engagement by: April 22nd, 2024 - May 17th, 2024

Summary

100% ⓘ OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
5	1	0	1	1	2

TABLE OF CONTENTS

1. Introduction
2. Assessment summary
3. Scope
4. Findings overview

1. Introduction

The `Trust Wallet team` engaged Halborn to conduct a security assessment on their smart contracts, beginning on April 22, 2024, and ending on May 17, 2024. The security assessment was scoped to the smart contracts inside their `amber-sc` GitHub repository, located at https://github.com/trustwallet/amber-sc, commit `5176f880cc40a6015af92ec1e456e87ec9725fb8`.

2. Assessment Summary

The team at Halborn was provided four weeks to review the codebase. The security engineer is a blockchain and smart-contract security expert with advanced penetration testing, smart-contract hacking, and deep knowledge of multiple blockchain protocols.

The purpose of this assessment is to achieve the following:

- Ensure that the system operates as intended.
- Identify potential security issues.
- Identify lack of best practices within the codebase.
- Identify systematic risks that may pose a threat in future releases.

In summary, Halborn identified several threats that were mostly addressed by the `Trust Wallet team`.

3. SCOPE

FILES AND REPOSITORY

(a) Repository: amber-sc

(b) Assessed Commit ID: 5176f88

(c) Items in scope:

- contracts/AmberGateway.sol
- contracts/standalone/StargateReceiver.sol
- contracts/libs/LibDiamond.sol
- contracts/libs/Core.sol
- contracts/libs/ReentrancyGuardian.sol
- contracts/facets/AssetManagerFacet.sol
- contracts/facets/DiamondCutFacet.sol
- contracts/facets/DiamondLoupeFacet.sol
- contracts/facets/OwnershipFacet.sol
- contracts/facets/dex/BaseDex.sol
- contracts/facets/dex/KyberSwapFacet.sol
- contracts/facets/dex/MimicSwapperFacet.sol
- contracts/facets/dex/OneInchFacet.sol
- contracts/facets/dex/ZeroExFacet.sol
- contracts/facets/bridge/AcrossV3Facet.sol
- contracts/facets/bridge/AllbridgeCoreFacet.sol
- contracts/facets/bridge/BaseBridge.sol
- contracts/facets/bridge/CCTPFacet.sol
- contracts/facets/bridge/SquidFacet.sol
- contracts/facets/bridge/StargateFacet.sol
- contracts/facets/bridge/SynapseBridgeFacet.sol

Out-of-Scope: contracts/libs/cBridge/Pb.sol, contracts/libs/cBridge/PbPool.sol, contracts/facets/bridge/CBridgeFacet.sol, contracts/facets/bridge/l2/ArbitrumOneFacet.sol, contracts/facets/bridge/l2/CBBaseFacet.sol, contracts/facets/bridge/l2/OptimismFacet.sol, contracts/facets/bridge/l2/PolygonPosBridgeFacet.sol, contracts/facets/bridge/l2/ZkSyncFacet.sol

REMEDIATION COMMIT ID:

- 475b771475b771
- 818e40a818e40a
- 38934023893402
- 02098890209889

Out-of-Scope: New features/implementations after the remediation commit IDs.

4. FINDINGS OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
HARDCODED DSTSWAPPER DOES NOT ACCOUNT FOR L2S WITH NON-COMPLIANT ADDRESS DERIVATION	CRITICAL	SOLVED - 05/15/2024
TEMPORAL FREEZING OF BRIDGED ETH WHEN USING STARGATE	MEDIUM	SOLVED - 05/15/2024
PASSING ZERO OR LOW DSTGASFORCALL WILL FREEZE FUNDS ON DESTINATION CHAIN TEMPORARILY	LOW	SOLVED - 05/15/2024
AMBERGATEWAY BYPASS BY CALLING STARGATE COMPOSER DIRECTLY	INFORMATIONAL	ACKNOWLEDGED
INCONSISTENCIES BETWEEN KYBERSWAPFACET AND MIMICSWAPFACET	INFORMATIONAL	SOLVED - 05/15/2024

Halborn strongly recommends conducting a follow-up assessment of the project either within six months or immediately following any material changes to the codebase, whichever comes first. This approach is crucial for maintaining the project's integrity and addressing potential vulnerabilities introduced by code modifications.