Smart Contract Security Audit Report

Socket (SuperBridge Integration)

1. Contents

2. General Information

This report contains information about the results of the security audit of the Socket.Tech (hereafter referred to as "Customer") SuperBridge route smart contract, conducted by Decurity in the period from 06/03/2024 to 06/04/2024.

2.1. Introduction

Tasks solved during the work are:

- Review the protocol design and the usage of 3rd party dependencies,
- Audit the contracts implementation,
- Develop the recommendations and suggestions to improve the security of the contracts.

2.2. Scope of Work

The audit scope included the following smart contract https://github.com/SocketDotTech/socket-ll-contracts/blob/feat/superBridge/src/bridges/superBridge/SuperBridge.sol. Initial review was done for the commit 9d4625fe267a3a7685bf32e5265b6277d6a9823b. The remediation review was done for the commit 256161e1b6f3755dcf0fc37e4f7981c6ca5f208c.

2.3. Threat Model

The assessment presumes the actions of an intruder who might have the capabilities of any role (an external user, token owner, token service owner, or a contract).

The main possible threat actors are:

- User,
- Protocol owner,
- Relayer,
- Token owner/contract.

2.4. Weakness Scoring

An expert evaluation scores the findings in this report, and the impact of each vulnerability is calculated based on its ease of exploitation (based on the industry practice and our experience) and severity (for the considered threats).

2.5. Disclaimer

Due to the intrinsic nature of the software and vulnerabilities and the changing threat landscape, it cannot be generally guaranteed that a certain security property of a program holds.

Therefore, this report is provided “as is” and is not a guarantee that the analyzed system does not contain any other security weaknesses or vulnerabilities. Furthermore, this report is not an endorsement of the Customer’s project, nor is it an investment advice.

That being said, Decurity exercises the best effort to perform its contractual obligations and follow the industry methodologies to discover as many weaknesses as possible and maximize the audit coverage using limited resources.

3. Summary

As a result of this work, we haven't discovered any exploitable security issues.

The other suggestions included fixing the low-risk issues and some best practices (see Security Process Improvement).

3.1. Suggestions

The table below contains the discovered issues, their risk level, and their status as of 05 June, 2024.

Table. Discovered weaknesses

Issue	Contract	Risk Level	Status
Broken tests	socket-ll-contracts/test/solidity/bridges/super-bridges/lyra/deposit.sol, socket-ll-contracts/test/solidity/bridges/super-bridges/lyra/withdraw.sol	Info	Fixed
Compilation error due to wrong NatSpec	SuperBridge.sol	Info	Fixed
Wrong comments	SuperBridge.sol	Info	Fixed
Absence of selectors	src/bridges/superBridge/SuperBridge.sol	Info	Fixed
UINT256_MAX can be private	src/bridges/superBridge/SuperBridge.sol	Info	Fixed

4. General Recommendations

This section contains general recommendations on how to improve the overall security level.

The Findings section contains technical recommendations for each discovered issue.

4.1. Security Process Improvement

The following is a brief long-term action plan to mitigate further weaknesses and bring the product security to a higher level:

- Keep the whitepaper and documentation updated to make it consistent with the implementation and the intended use cases of the system,
- Perform regular audits for all the new contracts and updates,
- Ensure the secure off-chain storage and processing of the credentials (e.g. the privileged private keys),
- Launch a public bug bounty campaign for the contracts.

5. Findings

5.1. Broken tests

Risk Level: Info

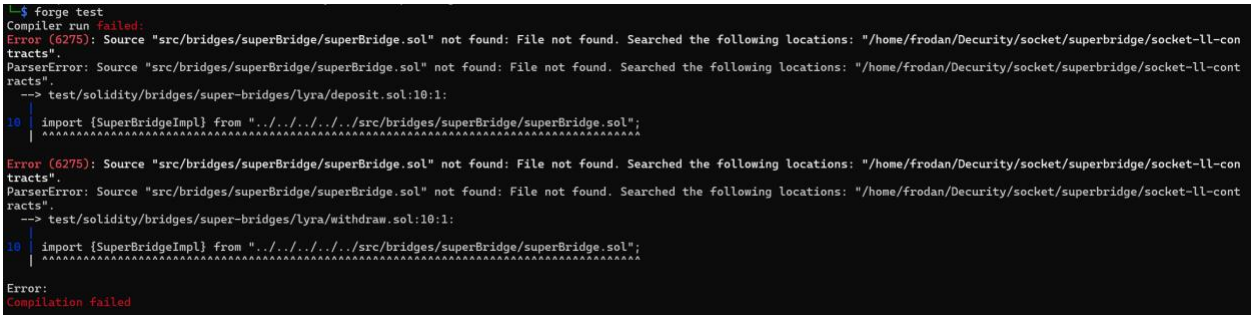
Status: Fixed in commit [2aa54e72](2aa54e72).

Contracts:

- socket-ll-contracts/test/solidity/bridges/super-bridges/lyra/deposit.sol,
- socket-ll-contracts/test/solidity/bridges/super-bridges/lyra/withdraw.sol

Description:

The tests for SuperBridge implementation have broken imports:



Broken import:

```
import {SuperBridgeImpl} from
"../../../../../src/bridges/superBridge/superBridge.sol";
```

Fixed variant:

```
import {SuperBridgeImpl} from
"../../../../../src/bridges/superBridge/SuperBridge.sol";
```

Remediation:

Consider fixing imports.

5.2. Compilation error due to wrong NatSpec

Risk Level: Info

Status: Fixed in commit 2aa54e72.

Contracts:

- SuperBridge.sol

Location: Lines: `227, 228`. Function: `swapAndBridge`.

Description:

The contract `SuperBridgeImpl` cannot be compiled because arguments of the function `swapAndBridge` doesn't match NatSpec. Specifically, the arguments do not contain described `metadata` and `receiver` parameters causing the compilation error:

```
[⠒] Compiling...
[⠒] Compiling 98 files with 0.8.15
[⠒] Solc 0.8.15 finished in 358.24ms
Error:
Compiler run failed:
Error (3881): Documented parameter "metadata" not found in the parameter list of the function.
   --> src/bridges/superBridge/SuperBridge.sol:219:5:
    |
219 |     /**
    |     ^ (Relevant source part starts here and spans across multiple lines).

Error (3881): Documented parameter "receiver" not found in the parameter list of the function.
   --> src/bridges/superBridge/SuperBridge.sol:219:5:
    |
219 |     /**
    |     ^ (Relevant source part starts here and spans across multiple lines).

Error (3881): Documented parameter "metadata" not found in the parameter list of the function.
   --> src/bridges/superBridge/superBridge.sol:219:5:
    |
219 |     /**
    |     ^ (Relevant source part starts here and spans across multiple lines).

Error (3881): Documented parameter "receiver" not found in the parameter list of the function.
   --> src/bridges/superBridge/superBridge.sol:219:5:
    |
219 |     /**
    |     ^ (Relevant source part starts here and spans across multiple lines).
```

Remediation:

Remove these arguments from NatSpec of the function

5.3. Wrong comments

Risk Level: Info

Status: Fixed in commit 2aa54e72.

Contracts:

- SuperBridge.sol

Location: Lines: `11, 24, 30, 47, 53, 75, 76, 126, 127, 159, 222`.

Description:

The contract `SuperBridgeImpl` has a number of comments written with typos:

- The word “keccack” should be replaced by `keccak`
- The word “tranfer” should be replaced by `transfer`
- The word “preceeding” should be replaced by `preceding`
- The word “receipent” should be replaced by `recipient`
- The word “briding” should be replaced by `bridging`

Remediation:

Fix these typos in comments

5.4. Absence of selectors

Risk Level: Info

Status: Fixed in the commit 256161e1.

Contracts:

- src/bridges/superBridge/SuperBridge.sol

Description:

The `SuperBridge` contract, unlike all other bridge implementations, does not define function selectors for its bridging functions. It may be beneficial to add function selectors to contracts for consistency.

Remediation:

Consider adding selectors.

5.5. UINT256_MAX can be private

Risk Level: Info

Status: Fixed in commit 2aa54e72.

Contracts:

- src/bridges/superBridge/SuperBridge.sol

Location: Lines: 21.

Description:

The variable `uint256 public immutable UINT256_MAX` can be private to save gas for the contract deployment.

Remediation:

Make the variable private.

6. Appendix

6.1. About us

The Decurity team consists of experienced hackers who have been doing application security assessments and penetration testing for over a decade.

During the recent years, we've gained expertise in the blockchain field and have conducted numerous audits for both centralized and decentralized projects: exchanges, protocols, and blockchain nodes.

Our efforts have helped to protect hundreds of millions of dollars and make web3 a safer place.