Cryptonics

SOLIDIFIED

Mobie Backend and Stellar Smart Contracts

Audit Report - September 24, 2020

Solidified Technologies Inc.
20 Ridgeview Ct
Sausalito, CA, 94965
UNITED STATES

https://solidified.io/

Cryptonics Consulting S.L.
Ramiro de Maeztu 7
46022 Valencia
SPAIN

https://cryptonics.consulting/

Table of Contents

Disclaimer

THE CONTENT OF THIS AUDIT REPORT IS PROVIDED “AS IS”, WITHOUT REPRESENTATIONS AND WARRANTIES OF ANY KIND.

THE AUTHORS AND THEIR EMPLOYER DISCLAIM ANY LIABILITY FOR DAMAGE ARISING OUT OF, OR IN CONNECTION WITH, THIS AUDIT REPORT.

THIS AUDIT REPORT IS NOT A SECURITY WARRANTY, INVESTMENT ADVICE, OR AN ENDORSEMENT OF THE CLIENT OR ITS PRODUCTS. THIS AUDIT DOES NOT PROVIDE A SECURITY OR CORRECTNESS GUARANTEE OF THE AUDITED SOFTWARE.

Summary of Findings

No	Description	Severity	Status
1	No Maximal Request Size Configured	Minor	Resolved
2	Unused Variable Declarations	Informational	Resolved
3	Incorrect Parameter Descriptions in Inline Endpoint Documentation	Informational	Resolved
4	Unused Dependency	Informational	Resolved

Introduction

Purpose of this Report

Cryptonics Consulting and Solidified have been engaged to perform a security audit of the Mobie payment service (https://mobie.io/). The engagement includes the blockchain-facing backend and smart contracts of the platform.

The objectives of the audit are as follows:

1. Determine the correct functioning of the backend, in accordance with the project specification.
2. Determine possible vulnerabilities, which could be exploited by an attacker.
3. Determine smart contract bugs, which might lead to unexpected behavior.
4. Analyze whether best practices have been applied during development.
5. Make recommendations to improve code safety and readability.

This report represents a summary of the findings.

As with any code audit, there is a limit to which vulnerabilities can be found, and unexpected execution paths may still be possible. The author of this report does not guarantee complete coverage (see disclaimer).

Codebase Submitted for the Audit

The audit has been performed on the code submitted in the following private GitHub repository:

https://github.com/implicitlabs/Mobile_Stellar_MBX

The following commit number was evaluated in the audit:

`76d31ce35855b92fd491d51768f4e12b7ddfdb42`

UPDATE: Fixes to the audit were submitted in final commit number:

`50ca7bbd5376df10af7884550b3489232919d4a0`

Methodology

The audit has been performed by two (2) independent auditors in the following steps:

1. Gaining an understanding of the code base's intended purpose by reading the available documentation.
2. Automated source code and dependency analysis.
3. Manual line by line analysis of the source code for security vulnerabilities and use of best practice guidelines, including but not limited to:
    a. Race condition analysis
    b. Under- / overflow issues
    c. Key management vulnerabilities
    d. Permissioning issues
    e. Smart contract logic errors
4. Report preparation

The results were then discussed between the auditors in a consensus meeting and integrated into this joint report.

Project Overview

The submitted code implements a backend that allows users to interact with the Stellar ledger. It supports the generation of keys, the transfer of Lumens, the transfer of a custom asset, the signing of transactions, and also implements an escrow functionality.

The API consists of an Express application and uses the Stellar Javascript SDK to connect to a Stellar Horizon API server.

The backend serves as a trusted intermediary between the end-user client and the Stellar platform. Whilst private keys are not stored by the API, they have to be supplied by the client in the API request and are sent to the server.

Findings

1. No Maximal Request Size Configured

Severity: Minor

The application does not limit the size of requests that can be received. A common denial of service attack scenario is flooding a server with very large requests. To protect against this it is recommended to limit the size of requests to a reasonable maximum.

Recommendation

Limit the size of the requests. For more detailed information, see the OWASP recommendations (https://cheatsheetseries.owasp.org/cheatsheets/Nodejs_Security_Cheat_Sheet.html#set-request-size-limits)

Update: A 1kb size limit has been added.

Status: Resolved

2. Unused Variable Declarations

Severity: Informational

In the `new-escrow` route definition in `src/controller/Stellar.js`, the public key of the sender is derived but never used:

```
const senderPublicKey =
stellarSdk.Keypair.fromSecret(senderSecretKey).publicKey();
```

Furthermore, the transaction result is obtained but not used.

Recommendation

Remove unnecessary public key derivation and consider returning the transaction result to the client.

Update: FIxed.

Status: Resolved

3. Incorrect Parameter Descriptions in Inline Endpoint Documentation

Severity: Informational

The parameter list in the comments for several endpoints in `src/controller/Stellar.js` seems to have been incorrectly copied and pasted incorrectly, leading to missing or wrong parameter descriptions.

Recommendation

Fix the parameter documentation.

Update: Fixed.

Status: Resolved

4. Unused Dependency

Severity: Informational

The `express-formidable` package is imported as a dependency but never used.

Recommendation

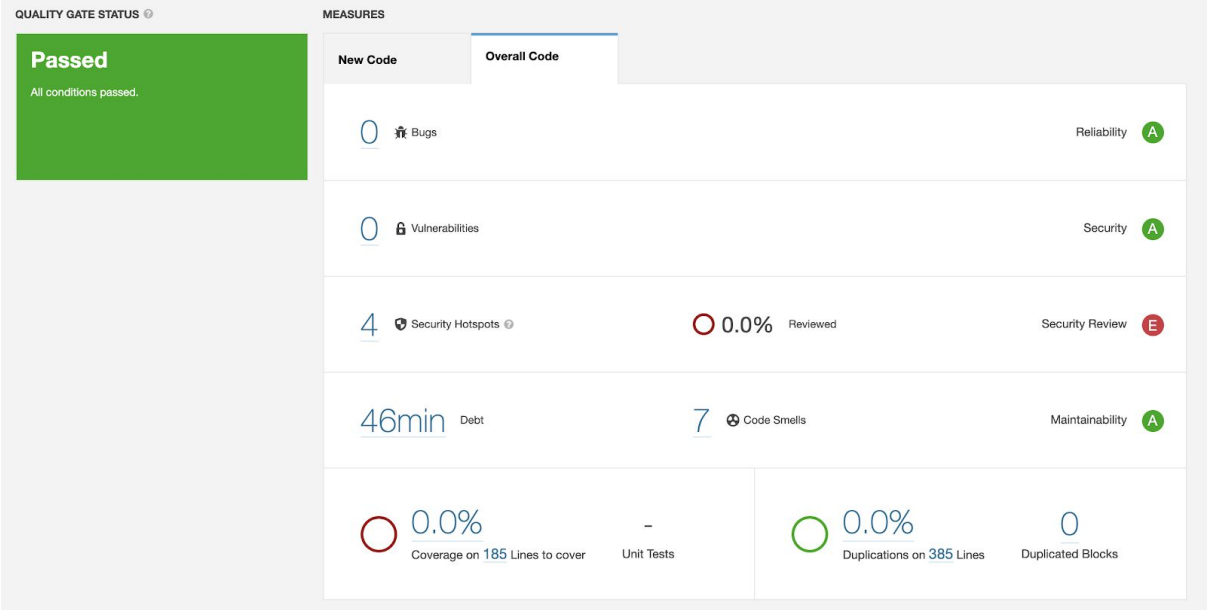
Remove unused dependencies.

Update: Fixed.

Status: Resolved

Appendix: Automated Code Analysis Report

sonarqube Analysis Overview



sonarqube Code Quality Issues

npm Dependency-Check

```
                    === npm audit security report ===


found 0 vulnerabilities

 in 188 scanned packages
```

njsscan Output

```
 njsscan --missing-controls Mobile_Stellar_MBX
- Pattern Match ████████████████████████████████████████████████████ 17
- Semantic Grep ██ 129

================================================================================================================
RULE ID: helmet_header_ienoopen
DESCRIPTION: Helmet IE No Open header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================================

================================================================================================================
RULE ID: helmet_header_xss_filter
DESCRIPTION: Helmet XSS Protection header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================================

================================================================================================================
RULE ID: helmet_header_hsts
DESCRIPTION: Helmet HSTS header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================================

================================================================================================================
RULE ID: helmet_header_dns_prefetch
DESCRIPTION: Helmet DNS Prefetch header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================================

================================================================================================================
RULE ID: helmet_header_referrer_policy
DESCRIPTION: Helmet Referrer Policy header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================================
```

```
================================================================================================
RULE ID: helmet_header_check_csp
DESCRIPTION: Helmet Content Security Policy header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================

================================================================================================
RULE ID: helmet_header_check_crossdomain
DESCRIPTION: Helmet X Permitted Cross Domain Policies header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================

================================================================================================
RULE ID: helmet_header_feature_policy
DESCRIPTION: Helmet Feature Policy header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================

================================================================================================
RULE ID: helmet_header_check_expect_ct
DESCRIPTION: Helmet Expect CT header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================

================================================================================================
RULE ID: anti_csrf_control
DESCRIPTION: This application does not have anti CSRF protection which prevents cross site request forgery
attacks.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-352: Cross-Site Request Forgery (CSRF)
================================================================================================

================================================================================================
RULE ID: helmet_header_nosniff
DESCRIPTION: Helmet No Sniff header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================

================================================================================================
RULE ID: helmet_header_x_powered_by
DESCRIPTION: Helmet X Powered By header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================

================================================================================================
RULE ID: rate_limit_control
DESCRIPTION: This application does not have API rate limiting controls.
SEVERITY: INFO
OWASP: A5: Broken Access Control
CWE: CWE-770: Allocation of Resources Without Limits or Throttling
================================================================================================
```

```
================================================================================================
RULE ID: helmet_header_frame_guard
DESCRIPTION: Helmet X Frame Options header is not configured for this application.
SEVERITY: INFO
OWASP: A6: Security Misconfiguration
CWE: CWE-693: Protection Mechanism Failure
================================================================================================
```