



# MPC application Source Code Review (updated)

FortVault LLC

June 2026



# Contents

|                                              |   |
|----------------------------------------------|---|
| MPC application Source Code Review (updated) | 1 |
| Background                                   | 2 |
| Scope                                        | 2 |
| General conclusion                           | 2 |
| Acknowledgment                               | 3 |
| Key Findings                                 | 3 |

# Executive Summary

## Background

In accordance with the [REDACTED] signed between FortVault LLC (furthermore the Client) and Grant Thornton Consulting CJSC, we have performed a security static source code review of the Clients's public facing environment.

A Code Review is a specialized task with the goal of identifying types of weaknesses that exist within a given code base. The task involves both manual and automated review of the underlying source code and identifies specific issues that may be representative of broader classes of weakness inherent in the code.

During the source code review, we've analyzed the source code for security issues and categorize the findings based on the weakness categories. Each finding is assigned a risk rating of Critical, High, Medium, or Low. This report presents the finding identified during the assessment.

The main objective of the assignment was to complete an independent security review of the MPC application source code and provide recommendations for actions necessary to strengthen the security and continuity of the application and reduce the likelihood of successful exploitation.

## Scope

The scope of this assessment included the backend source code of the MPC application provided by FortVault representatives.

The review covered key components of the application, including database interaction logic, configuration handling, and credential management within the codebase.

## General conclusion

The source code review initially identified [REDACTED] related to [REDACTED]. Based on the remediation evidence provided by the Client, [REDACTED] was removed from the source code. As a result, [REDACTED] is considered remediated and no material security findings remain open.

For systems to remain secure, security posture must continue to be evaluated and improved on an ongoing basis. The Client should maintain [REDACTED] practices and continue using [REDACTED] mechanisms to prevent [REDACTED] in the source code.

## Acknowledgment

We would like to take this opportunity to thank the Client's management and staff for their cooperation during this assignment.

## Key Findings

| Area/Risk              | Critical | High | Medium | Low |
|------------------------|----------|------|--------|-----|
| Application Assessment | -        | -    | -      | -   |
| Vulnerabilities        |          |      |        |     |



© 2026 Grant Thornton Armenia. All rights reserved.

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton Armenia is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms.

GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.