mnemonic

Confidential

Report Summary
Security Assessment
Firi AS

Place	**Oslo, Norway**
Date	**2024-12-20**
Version	**1.0**
Author	**Alexander Evans, Andreas Claesson, Anna Rozanska**

Executive summary

In November and December 2024, mnemonic performed a security assessment of the Firi platform. The platform is used for crypto coin trading, it is written in a mixture of GoLang and TypeScript, providing multiple front-ends for their customers. Amongst the front-ends exist mobile clients and a web platform.

This report documents the testing of the web application front-end, its respective back-end API and a code-review of the entire platform. Additionally, in combination with the above listed documented coverage and activity, an assessment into the Firi platform cloud infrastructure and IAM was performed in parallel, which is documented in a separate report.

The main goal of the test has been to identify concrete vulnerabilities and provide advice about how these vulnerabilities can be fixed or mitigated. This has been achieved by providing an independent security review of Firi software and supporting infrastructure. Obtaining more insight into their overall security status of the application, assists to select and prioritize remediation activities in order to manage overall risk exposure.

Secondary goals of the project have been to increase awareness within Firi about software security and vulnerabilities, and to provide documentation that an external technical security assessment has taken place.

Testing has been carried out from mnemonic's dedicated testing environment in Oslo, by experienced security consultants. Dedicated test accounts and test teams were used in order to avoid exposure of customer data.

This technical report describes the findings and observations made during the assessment, as well as recommendations and potential improvements.

Summary of findings

mnemonic scores findings and vulnerabilities from the security assessment on a scale from 0-4, where 4 is critical and 0 is informational. During the assessment, we documented a total of 12 individual findings within the report. No [4-Critical] or [3-High] severity findings were observed during testing and the code review. Of the residual findings 2 were deemed as of [2-Medium] severity, 8 of [1-Low] severity and the rest are informational.

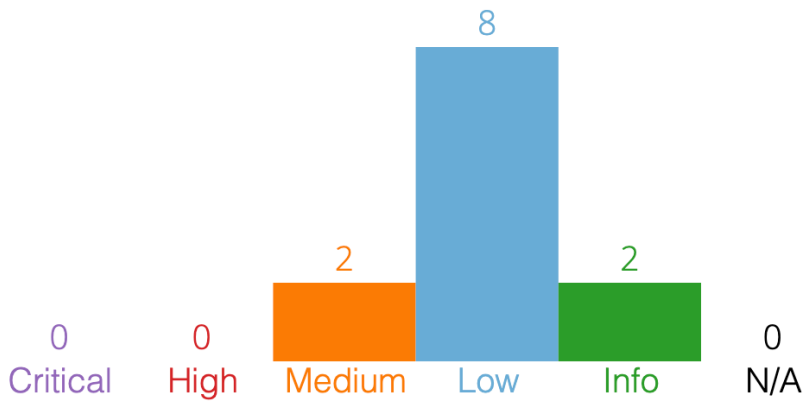

Diagram 1: An illustration of findings and their severities.

The low severity findings revolve around deviations in defense in depth and security best practices. These types of findings constitute configuration issues, observations and other artefacts that could impact the security of the scoped system when left unattended, unforeseen circumstance and scenarios of very low likelihood.

Summary of recommendations

For each of the identified improvement areas, mnemonic has provided multiple recommendations for how to improve the security posture of the Firi application.

Low severity findings should be reviewed as-is and quick wins gathered whilst applying contextual knowledge and risk valuation. mnemonic encourages Firi to review each finding based on their knowledge of their business context, internal and external requirements, risk appetite, and other constraints.

The report provides guidance on how to address the security weaknesses, as well as the other findings. Implementing these changes will significantly increase the general resiliency against cyber-attacks.

Test Execution

mnemonic tested for standard web application vulnerabilities, such as those listed in the OWASP Top 10 Application Security Risks.

The security assessment simulated a knowledgeable and skilled threat actor attempting to explore the system, bypass the security controls present, or otherwise cause undefined or unexpected behavior.

Testing was conducted remotely from mnemonic’s headquarters in Oslo, Norway.

Testing Methodology

mnemonic has conducted security and penetration testing, source code audits, and related services, ever since the company was founded in 2000. Our security testing methodology is based on the combination of open standards and collections of "industry best practice", together with our own experience accumulated over the last 20 years. In addition to this, testing is supported by an extensive knowledge base, as well as internally developed tools and scripts.

Our methodology is supported by the processes "*P3003 Procedure for security testing*" and "*P3006 Use and maintenance of testing platform*" in mnemonic’s ISO 9001 / ISO 27001 certified quality and security management system, as well as associated templates and documentation.