mnemonic

Confidential

Report Summary
AWS Security Assessment
Firi AS

Place	**Oslo, Norway**
Date	**2024-12-20**
Version	**1.0**
Author	**Andreas Claesson**

Executive summary

In November and December 2024, mnemonic was contracted by Firi AS to perform a security assessment of their AWS environment. Another part of the assignment was a security test of the Web application, as well as a review of the source code. These activities are described in a separate report.

The goal of the assessment is to provide an independent technical quality assurance of the environment, while making recommendations for improvement areas which can help increase the overall security posture of the deployment.

mnemonic has first focused on the following core areas of the environment: Identity and Access Management (IAM), and Cloud network architecture. These areas are regarded as the very foundation of every cloud deployment, since insecure architecture and strategy might impact the business beyond the applications hosted in the environment.

The second part of the assessment has focused on reviewing AWS resources for potential misconfigurations (including secrets management and logging strategies), as well as assessing the external network attack surface of the environment.

Both parts of the assessment have been conducted remotely from mnemonic's headquarters in Oslo, directly against Firi's AWS environment. This technical report describes the in-depth findings and observations made during both parts of the assessment, associated with mnemonic's 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 severity and 0 is informational.

In total, mnemonic has discovered 15 security issues, of which two have an estimated medium severity, and 11 with low severity. We have also included two informational findings.

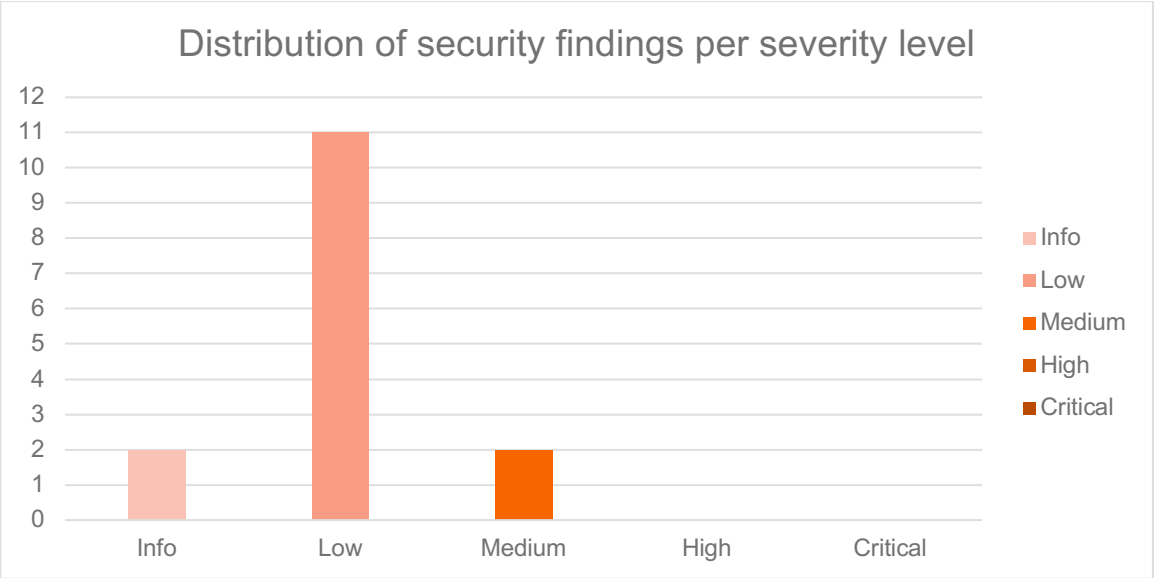

Figure 1: Distribution of security findings per severity level.

The assessment has revealed that Firi is affected by security issues related to mainly four areas:

1. Identity and Access Management (IAM)

IAM is regarded as the most sensitive area of a deployment, as any security issue belonging to this area typically affect multiple, if not all Cloud applications in the deployment. In general, the IAM strategy at Firi is robust and appears to be well thought through. The low severity findings should be considered as an extra layer of security, and best practice recommendations.

2. Cloud networking

Cloud networking is affected by four findings with an estimated low severity. The network architecture is well planned, and the findings are to be regarded as best practice recommendations.

3. Hardcoded secrets

Storing secrets in any environment is always difficult as it requires a balance between security and usability. We found two issues with an estimated low severity where Slack webhooks were stored. The impact of these issues is very low, but as a general rule to minimize the blast radius of an attack, secrets should always be handled by native secret storage like AWS Secrets Manager.

4. Configuration hardening

Configuration hardening is the most common area of cloud vulnerabilities, since it reviews the configuration of all cloud components. In this area we found two issues with medium severity, and three issues with low severity.

Summary of recommendations

The medium severity issues should be addressed first, as they are the most concerning issues, and could be mitigated with little effort.

Regarding the low severity issues, we recommend prioritizing removing all hardcoded secrets, and replace them with AWS Secrets Manager or similar.

For the rest of the issues, we recommend prioritizing improvements based on risk and information classification according to Firi's information security management system, as well as their knowledge of business context, internal and external requirements, risk appetite, and other constraints.

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.