Forta AirDrop Assessment - Audit Report

April 13th, 2022

Provided to:

Forta

by:

dédalo

www.dedalo.io - info@dedalo.io

Table of Contents

OVERVIEW

Forta engaged Dédalo's team to conduct a white-box security audit of Forta AirDrop and its source code. This process consisted of identifying possible threats and security risks in the components of Forta AirDrop source code and its infrastructure. Dédalo performed source code reviews, manual and dynamic tests with multiple tools and techniques to identify security weaknesses. To properly test AirDrop components, we performed tests locally and also in a staging environment provided by Forta.

Every finding is described in this document, including details that we consider necessary to understand the dangers of their possible impact, along with proper recommendations.

SCOPE

This assessment was done on the source code of the “Forta AirDrop” application provided by Forta through two private GitHub repositories.

The following components were delivered to Dédalo and have been audited:

- GitHub repositories:
  - `airdrop-interface`
  - `airdrop-api`

- Forta AirDrop staging environment:
  - **`airdrop-api-dev.forta.network`**
  - **`staging.airdrop.forta.network`**

EXECUTIVE SUMMARY

For this audit, we analyzed all the components of Forta AirDrop specified in the scope, and we couldn't identify security vulnerabilities that negatively affect Forta's business and users' data. This security assessment was conducted between Jun 7, 2022, and Jun 10, 2022, and the following days were used for findings triaging and report elaboration.

We thoroughly reviewed source code from both interface and API for Forta Airdrop, looking for misconfigurations, and incorrect input sanitizations, among other security issues that may arise.

In our dynamic penetration testing stage, we tested the rewards mechanics with the flows for rewards by Github users and addresses, constantly examining every input/parameter and attack vector.

In conclusion, we couldn’t find any security-related issues to report besides the absence of common security headers. In the airdrop-interface repository, we noticed the existence of legacy code. We recommend removing unused code from the Airdrop front-end to narrow the possibility of attack vectors.

WORK TEAM

The work team assigned to this project consisted of the following qualified roles:

- 1 Project Leader
- 2 Security Analysts

The Project Leader acted as the direct communication link between Dédalo and the client, resolving all doubts and providing the client with information and updates on the project, according to the times required by it. Simultaneously, he coordinated and provided support to the Security Analysts, which were responsible for carrying out the operative tasks that the security assessment process involved.

METHODOLOGY

Our security analysis methodology is based on the industry standards OWASP Testing Guide v4, OWASP Docker Security rules (for container-based systems), and OSSTMM (Open Source Security Testing Methodology Manual). For this project, we used a hybrid approach of penetration testing techniques against Forta Airdrop staging environment for dynamic testing combined with manual source code review on the provided Forta Airdrop repositories.

TECHNICAL REPORT

SECURITY ISSUES

We found the following issues classified by severity level:

#01 - Lack of Security Headers

Severity: Low

Description

The web application lacks the following set of recommended security headers and configurations:

- **Content Security Policy (CSP):** Helps prevent common client-side attacks like Cross-Site Scripting (XSS)
- **X-Frame-Options (XFO):** Helps prevent ClickJacking attacks.
- **X-XSS-Protection**: Helps to protect against JavaScript injection attacks through cross-site scripting.

Recommendations

It is recommended to configure these HTTP Headers to effectively prevent Client-side attacks.