

Vulnerability Assessment Report

Copyright © 2023 Security Pattern s.r.l. - All Rights Reserved

This document is private and confidential - Subject to N.D.A.

<i>Revision</i>	<i>Author</i>	<i>Date</i>	<i>Notes</i>
v01	S. Cristalli	2023/07/19	Version released to the client

1. Introduction

40 Factory has developed a cloud platform for managing IoT installations for clients, and gathering/displaying data from the devices. The main functionalities are offered through a web application to end clients.

Security Pattern has conducted a Vulnerability Assessment activity on the web platform, with the aim of identifying any vulnerabilities that could potentially affect the security of the entire system.

The analyses done by Security Pattern have covered the following areas:

- Interfaces of the 40 Factory platform with the outside world
- Perimeter of the web application and of its API
- Authentication mechanisms

The assessment activities have been executed between 2023/03/07 and 2023/07/14.

The assessment has been conducted on two separate platforms, namely Microsoft Azure and Mindsphere, both hosting the same web application.

1.1. Scope

The testing scope of the web application included two separate environments:

- An environment deployed on Microsoft Azure
- An environment deployed on Mindsphere

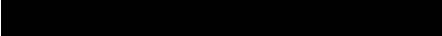
Security Pattern tested the two environments separately; each environment has its own results section in this document. Below we report the high-level information about each environment:

1.1.1. Microsoft Azure

Endpoints:

- Web application: <https://matdemo.40mat.com>

Users:

- 
- 

1.1.2. Mindsphere

Endpoints:

- Web application: <https://mswitops-mcctestenv-fortyops.eu1.mindsphere.io>

Users:

- [REDACTED]
- [REDACTED]

1.2. Methodology

For their Vulnerability Assessment activities, Security Pattern follows a mixed approach, with both automated and manual tests.

For designing and selecting the specific tests, their relevance is evaluated in comparison with industry-standard guidelines, such as the ones from OWASP; in particular, the tests from the OWASP Web Security Testing Guide are taken into consideration. Also, the selection of tests is always adapted to the particular target being tested; Security Pattern is making sure that the tests are suitable for the system, with an *ad hoc* evaluation of:

- documentation about the system received from the client
- information about the system discovered by Security Pattern experts during testing
- the agreed perimeter for the assessment activities

For the testing of the 40 Factory Web Platform, Security Pattern has performed tests that include, but are not limited to, the following categories and items:

- Information gathering
 - HTTP header analysis
 - Cookie analysis
 - Entry point identification
 - Collection of relevant API and resources
 - Functional mapping of web application
 - Information disclosure by errors
- Authentication/authorization
 - Testing of authentication mechanisms
 - Tests on JWT tokens
 - Analysis of roles and permissions
 - Privilege escalation
- Session management
 - Session timeout
 - Logout management
- Data validation testing
 - Reflected XSS
 - Stored XSS
 - SQL injection
 - HTTP parameter pollution/manipulation
- Error handling
 - Analysis of error codes
 - Analysis of error messages
- Business logic testing

- Business logic data validation
- Integrity checks
- Abuse of functionality
- File upload vulnerabilities
- Cryptography
 - Testing of proper TLS configuration

The tests performed by Security Pattern are extensive, focusing on *breadth* and *coverage* (i.e. trying to find a high number of vulnerabilities in the various aspects that compose the target's security, without leaving any part not analyzed). However, it is worth noting that the results of this vulnerability assessment cannot guarantee *completeness*; namely, it is not possible to guarantee the absence of:

- any vulnerability with a type that has not been found in this assessment
- vulnerabilities that are similar to the ones that have been found in this assessment

Regarding the second point, given the fact that single vulnerabilities can indicate the presence of underlying design or implementation flaws, it is strongly suggested to review the vulnerabilities that have been identified and to correct the underlying causes, searching for other entry points where the same issues could potentially be present.

To evaluate the impact of detected vulnerabilities, Security Pattern adheres to the criteria used within the CVSSv3 scoring system. In this document, the qualitative evaluation associated with each vulnerability is reported. The table below summarizes the meaning of each severity level.

Level	Description
CRITICAL	<p>Vulnerabilities which impact the entire system, and which can compromise its essential functions.</p> <p>Attackers (even if inexperienced) can easily exploit these vulnerabilities to cause damage.</p> <p>It is strongly recommended to take immediate corrective actions.</p>
HIGH	<p>Vulnerabilities which impact large portions of the system, and which can compromise its essential functions.</p> <p>Attackers with some experience can easily exploit these vulnerabilities to cause damage.</p> <p>It is recommended that corrective actions for resolution are planned to be executed within a few days.</p>
MEDIUM	<p>Vulnerabilities which impact restricted portions of the system, and which can compromise its essential functions.</p> <p>It is possible that, under the right conditions, expert attackers may exploit these vulnerabilities to cause damage.</p> <p>It is recommended that corrective actions for resolution are planned to be executed within a few weeks.</p>
LOW	<p>Vulnerabilities which impact restricted portions of the system, and which cannot singularly impact its essential functions.</p> <p>It is possible that, under the right conditions, expert attackers may exploit these vulnerabilities to cause damage; however, such an event is expected to occur with low likelihood.</p> <p>It is recommended whether it is necessary to take corrective actions for resolving these problems, evaluating the system context and its threat modeling.</p>
INFORMATIVE	<p>These items do not represent vulnerabilities per se, but rather inform about implementation choices for which some improvement is possible (referring to industry best practice).</p> <p>It is recommended whether it is necessary to take actions for implementing the suggested improvements, evaluating the system context and its threat modeling.</p>

2. Results

Security Pattern has executed three rounds of vulnerability assessment on the web platform.

After every iteration, the results have been shared with 40Factory, which has performed the adequate corrective actions.

At the end of the testing activities, Security Pattern reports no relevant vulnerabilities.
Vulnerability summary:

CRITICAL: 0

HIGH: 0

MEDIUM: 0

LOW: 0

INFORMATIVE: 0