Computest

**Partner Security Quickscan**
E-Progress B.V.

>>

# WE EAT SECURITY FOR BREAKFAST.

June 26, 2023
Abdul Rahman Mhimid Dbis

# Summary

Computest conducted a security Quickscan for E-Progress on 22 and 23 of June 2023. Computest' security specialist Abdul Rahman Mhimid Dbis have spoken with E-Progress' consultant and product owner Froukje de Jong, Charissa Kiezebrink and Blue Coded's senior developer Jarl Ilbrink about the security of the i-Talent software.

The main goal of the Quickscan is to provide an insight into the security level of the E-Progress' i-Talent software. This document therefore only gives a general impression and is not a complete list of all security issues in the tested platform.

The i-Talent software supports the entire process of performance and talent management. It offers tools to connect organization, teams and individuals. The software is built around four modules: strategy & strategic personnel planning (SPP), goals & actions, portfolio and academy.

The software is developed using C# and makes use of the Microsoft ASP.NET framework. The application is deployed on IIS server and self-hosted. Furthermore, the application makes use of various JavaScript libraries to deliver different functionalities to the end user.

During the Quickscan, Computest focused on the security of the i-Talent application from different aspects such as security in the development process, security in code and security in practice to provide insight into its security level and whether the tested software poses risk to AFAS.

## Result

Scores have been granted to the four categories mentioned below. Each of these categories will be explained further in this document.

| Scores | |
|---|---|
| **Security in the development process** |  |
| **Security in code** |  |
| **Security in practice** |  |
| **Risk for AFAS** |  |

The risk for AFAS is given a green traffic light. The security level of the tested application is estimated at relatively high. Therefore, a new security Quickscan will be planned after three years.

## Security in the development process

There is sufficient attention to security in the development process

The i-Talent platform has been developed with security in mind. E-Progress uses Jira as a ticketing software for organizing tasks and implementing new features to the application. Next to this, Azure DevOps is being used as a version control system. Although access to Azure DevOps requires a VPN access, multi-factor authentication (MFA) is not enforced for extra protection. Different branches and environments are being used for development, testing, acceptance and production. Access to these environments is protected by a firewall. Therefore, only allowed users are able to obtain access to these environments.

The platform utilizes OWASP Dependency-Check in the CI/CD pipeline to detect publicly disclosed vulnerabilities contained within the platform's dependencies. In addition, code reviews are enforced prior to pushing a new code to production through Jira and only senior developers can perform this task. However, there is no static or dynamic security testing (SAST & DAST) implemented in the pipeline to detect potential vulnerabilities that might be present in the source code.

Within the platform, a new isolated environment will be deployed for every E-progress' client. Sensitive data of a client such as employee/manager full name, email, job title and start date is stored in a separate database. Access to the database server is protected by a firewall and not externally accessible. Additionally, AFAS API token is stored encrypted (AES-256) on a different server and a background process is used to sync data through the AFAS GET Connector.

Security policies on developers' workstations are enforced through group policies. All developers' workstations have full disk encryption enabled via BitLocker. Add to that, Windows Defender is enabled and regularly updated. Furthermore, clear screen and disk policy are also enforced. Moreover, Passwordstate is used by developers for password management.

No definitive vulnerability disclosure policy is currently in place. However, vulnerabilities will be addressed by the senior developers and will be prioritized based on their impact.

Computest advises the following:

- Enforce MFA on all environments that are used in the development process;
- Implement SAST and DAST methodologies in the CI/CD pipeline;
- Require developers to follow secure code trainings;
- Establish a definitive procedure to resolve a security vulnerability;
- Conduct periodic security tests by an independent third-party;
- Draw up a vulnerability disclosure policy (VDP).

## Security in code

There is sufficient attention for security in the application's source code

Computest reviewed parts of the source code of the i-Talent platform that is related to sensitive functionalities such as authentication and authorization, user input handling and the general structure of the source code together with the developer.

The platform is developed using C# and makes use of the Microsoft ASP.NET framework for the backend and React framework for the frontend. The codebase is structured based on modules implemented within the platform and follows the MVC pattern. In addition, descriptive comments are present in parts of the source code and the functions written were short and self-explanatory. Error handling, authentication, authorization, cross-site request forgery protection and other security related measures are implemented in a centralized way. Furthermore, the .NET entity framework is used to protect the web application against SQL injection attacks. Add to this, the Razor view engine used in MVC automatically encodes all output sourced from variables to prevent cross-site scripting attacks.

Although the application is well protected against different attack types, Computest found that protection against brute-force attack is improperly implemented and can lead to lockout the user account if the attacker submits three invalid login attempts. Computest recommends replacing the lockout mechanism with a strong CAPTCHA.

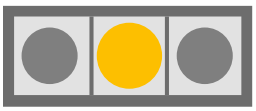
Additionally, the admin environment offers a functionality that allows admins to modify users' information such as first and last name. Computest found that the Razor syntax is not used to encode the first name of the user. Therefore, an attacker who has access to an admin account can abuse this functionality to inject malicious HTML code into the email body to alter its content. This could allow an attacker to trick the user to visit a malicious website to potentially steal the user's credentials. The exploitation of this security issue is hard as the attacker needs to have access to the internal/VPN network and valid admin credentials.

Lastly, Computest identified a potential security issue where the value of the ReturnUrl and RedirectToAction parameters might not be well validated which makes the application potentially vulnerable to open redirection.

Computest advises based on the above:

- Replace the lockout mechanism with a strong CAPTCHA;
- Ensure that user input is escaped everywhere in the output of email messages;
- Ensure the URL submitted by the user in the ReturnUrl and RedirectToAction parameters is properly validated.

## Security in practice



There is insufficient attention for security in practice

Computest carried out a short security test on the acceptance environment of the i-Talent platform on the 23rd of June 2023. The acceptance environment was indicated by E-Progress to be representative of the production environment. The security test was mostly focused on the authentication mechanism, possible injection attacks and security issues that could introduce a security threat.

Computest identified three security issues within the platform from medium to low impact. The discovered vulnerabilities were related to session management and third-party software. It was found that the user's session is not immediately revoked after the user logs out of the application. In addition, the user's session is not regenerated or revoked after the user changes his password. Therefore, it is possible for an attacker who somehow obtained the user's session to perform actions in the context of the user and without the user's consent even if the user logged out of the application and/or modified the password.

A cross-site request forgery has been identified in this test. To logout the user from the application, a GET request will be sent. As the logout done in a GET request with no additional verification of the origin, an attacker can abuse this vulnerability to keep the user logged out of the application.

Additionally, the i-Talent platform makes use of various JavaScript libraries such as jQuery UI, jQuery validation, jQuery datatables, moment and Bootstrap. The used version of the third-party libraries found to be outdated and vulnerable to prototype pollution, cross-site scripting (XSS) and regular expression denial of service (ReDOS). Moreover, the bootstrap library is obsolete and not supported anymore by the vendor. Therefore, newly discovered security vulnerabilities will not be patched and might leave the platform vulnerable to different type of attacks. Computest was could not exploit the security issues of the libraries used due to the limited time of this security test.

Computest advises the following:

- Revoke the user's session immediately after the user's logs out;
- Regenerate and revoke the user's session after the user changes the credentials;
- Verify the origin of the logout request;
- Ensure that third-party software is always up-to-date.

## Risk for AFAS

The security risk for AFAS is estimated at ‘Low”.

The i-Talent platform of E-Progress is developed using modern and well-known frameworks that provide security measures against common vulnerability types. Next to this, sensitive information obtained from AFAS are securely stored as each customer has a separate and isolated database. The database is only accessible by developers and protected behind a firewall. The AFAS API token is stored on a different isolated server and encrypted using the AES-256 algorithm.

The platform provides proper protection against vulnerabilities that could introduce direct security risk to AFAS API token. Computest has therefore estimated the risk for AFAS as ‘Low’.