Policy extract vulnerability remediation

Identified vulnerabilities detected in production systems or applications are to be remediated according to the following vulnerability remediation baselines:

Risk level	Remediation baseline
Critical	Immediately
High	60 days
Medium	180 days
Low / info	If relevant, to be remediated at discretion of Product Owner

Pentest 2022: myProtime

Context

Protime & SD Worx have requested Toreon to perform a grey box web application penetration test on the myProtime application between 01/12/2022 and 07/12/2022. This application serves as a time & attendance self service module.

The objective of this test was to discover any security vulnerabilities residing in the application. This report provides Protime & SD Worx with an overview of all identified vulnerabilities and defines measures to optimize the security of the application components.

Observations Toreon

We were unable to perform unauthorized operations such as gaining unintended access to other client data and settings on all in-scope application components. Furthermore, the application properly mitigated a wide range of attacks such as injection, privilege escalation, directory traversal, etc.
The infrastructure components and third-party software used, have a good reputation with regard to security. Lastly, an external vulnerability scan on the infrastructure showed no significant weaknesses. There are no unneeded ports/services or interfaces available and active.

Management Summary

Overall security rating

Critical findings

No critical vulnerabilities.

High findings

No high vulnerabilities.

Medium findings

M.1.: More information available upon request.

Low/informational findings

L.1.: Known Vulnerable or Outdated Package

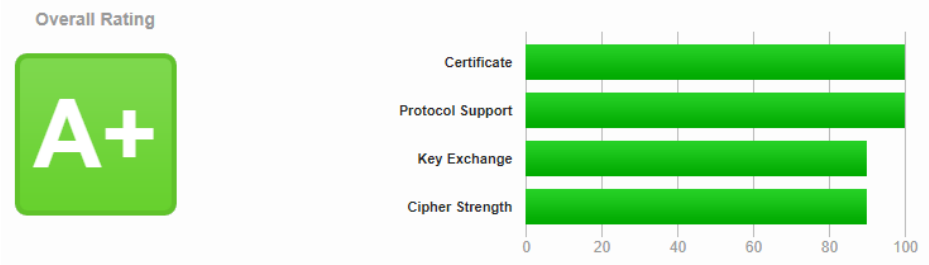
Protime action plan: Outdated library will be replaced by a new version. First experiments on-going but currently no commitment on timing.

L.2.: Content Security Policy Misconfiguration

Protime action plan: Investigate the use of properly configured Content Security Policies as an additional defensive measure for protecting the application and its users. The unsafe-eval directive will be fade out on all pages (except the myProtime people page). The unsafe-inline directive needs further investigation before any commitment on timing.

I.1.: TLS/SSL Settings are not secure

Protime action plan: No action plan needed as SSL Labs score is A+. SSL Server Test: myProtime.eu (Powered by Qualys SSL Labs)



External pentest company

Toreon CVBA
Grotehondstraat 44 1/1
B-2018 Antwerpen
Belgium

T +32 (0)33 69 33 96
M info@toreon.com

Version control

Date	Author	Comment
24/02/2023	Bert Van Doorsselaere, Teamlead Cloud Technologies	Action plan documented