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: Protime Premium

Context

SD Worx and Protime have requested Toreon to perform a grey box web application penetration test on Protime Premium between 07/11/2022 and 16/11/2022. Protime Premium is a time & attendance application in which absence and presence of employees can be managed.

The objective of this test was to discover any security vulnerabilities residing in the web application. This report provides SD Worx and Protime 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 customer data, databases or servers and other in-scope application components. Furthermore, any type of injection attack in the authenticated part of the application was successfully mitigated.

Management Summary

Overall security rating

Critical findings

No critical vulnerabilities.

High findings

No high vulnerabilities.

Medium findings

M.1.: Reflected Cross Site Scripting

Protime action plan: Affected component will be replaced by May 2023.

Low/informational findings

L.1.: Content Security Policy Misconfiguration

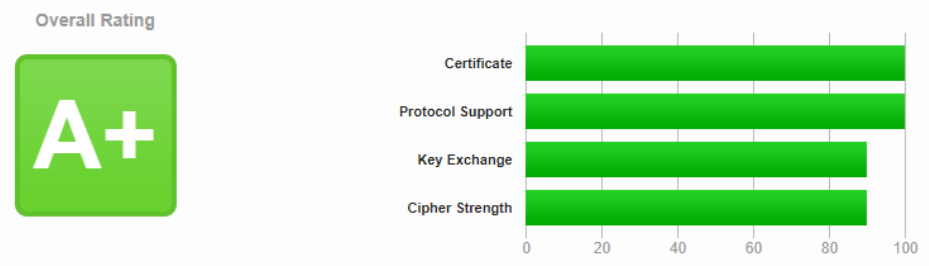
Protime action plan: Investigate the use of properly configured Content Security Policies as an additional defensive measure for protecting the application and its users.

L.2.: Server response headers disclose information

Protime action plan: Affected component will be replaced by May 2023.

L.3.: TLS/SSL Settings are not secure

Protime action plan: Low finding is considered informational as SSL Labs score is A+ SSL Server Test: myProtime.eu (Powered by Qualys SSL Labs)



I.1.: Strict Transport Security Policy Misconfiguratio

Protime action plan: HTTP Strict-Transport-Security (HSTS) header was set twice in the server responses. Will be solved by the end of 2023

I.2.: Cookie Without HTTPOnly Flag Set

Protime action plan: Cookies do not have the HTTPOnly flag set. Will be fixed with the new Parallels version rollout. Currently no commitment on timing.

I.3. Cookie With Secure Flag Missing

Protime action plan: Will be fixed with the new Parallels version rollout. Currently no commitment on timing.

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