Third party memo

Security test Testmonitor

Client Name:	Testmonitor
Main Contact:	René Ceelen
Audited by:	Vest Information Security
Main Contact:	Ruben Smit
Supervised by:	Marc Hullegie
Date:	27-10-2020
Status:	Final
Versie:	1.0
Classification:	**Confidential**
Subject:	Security test Testmonitor
Reference:	P501739
Iteration:	1DA

Security test – Testmonitor

Version: 1.0
Status: Final
Confidential
Datum: 27-10-2020

1. Management summary and conclusion

This TPM statement describes in general the findings and recommendations of the technical information security assessment, as performed by Vest on the test environment of Testmonitor during test iteration 1DA, in the period of 12-10-2020 to 22-10-2020.

Information security as a whole comprises three well-known areas: confidentiality, integrity and availability. This security test focuses on technical vulnerabilities with respect to violations of confidentiality and integrity of information (systems).

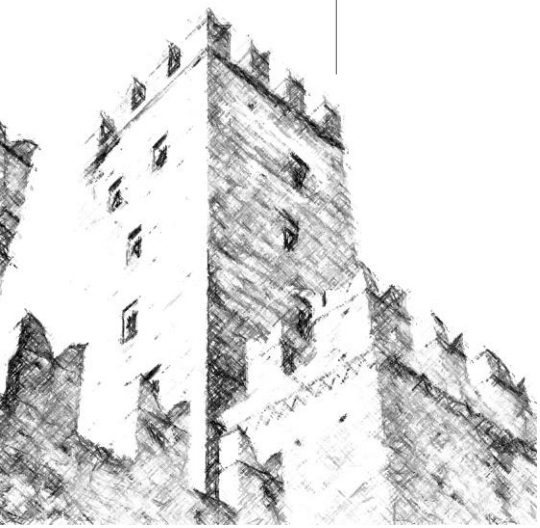
This security assessment resulted in several findings which have already been assessed in context by Testmonitor. The findings and recommendations are evaluated by a color and label indicating the risk evaluation-areas: “high”, “medium” and “low”. Any additional information is colored blue and labelled “informational”. In order to evaluate the risks, Vest uses a methodology based on the OWASP Risk Rating framework

The following table contains the number of identified vulnerabilities:

FINDINGS	RISK EVALUATION			
	High	Medium	Low	Info
Amount	0	3	1	1

It is recommended to address ‘high’ risks within a week. The risks evaluated as ‘medium’ risks are advised to address within a month and risks evaluated as ‘low’ within 3 months. Blue labelled informational findings do not need to be resolved or cannot be resolved.

This document contains a summary of the recommendations and a conclusion. Detailed findings are described in more depth in the comprehensive report on this security test.



2. Recommendations

For each of the findings a detailed description and recommendation can be found in the extensive report on this security test.

To assess the business impact of the found technical vulnerabilities, thorough knowledge of the organization is required. In general risks need to be placed in context of business impact. This is especially applicable in the communication with management. In the end the risk for the organization justifies investments in security measures. Many organizations have an overview of possessions (physical and non-physical) and their value to the organization and/or a business impact reference table to determine what is important to the organization. These sources of information can contribute to determine what is truly import for security.

3. Conclusion

The security of Testmonitor is estimated very positively. The findings found could be remedied relatively easily. Testmonitor clearly uses most security best practices and takes its security very seriously.

Vest is very satisfied with the security, but believes that by following the recommendations, Testmonitor can develop an even better security profile.

Naarden, 27-10-2020

Vest Information Security

Version: 1.0
Status: Final
Confidential
Datum: 27-10-2020