COMPREHENSIVE SECURITY TEST[1] No 4

BACKGROUND INFORMATION[2]:	
Related reform	3.5 Reconfiguration of basic digital services and safe transition to cloud infrastructure
Target name	58. Central security testing of public authorities' information systems
Target description	Number of comprehensive security tests carried out by the Information System Authority – the test results shall be summarised in reports.
The test was financed by the European Union from the NextGenerationEU Recovery Fund.	

PENETRATION TESTING INFORMATION:	
Date / period of testing	24.10.2023 – 01.11.2023
Objective of the Penetration Testing	Detect vulnerabilities in new public internet kiosk solution
Approach, Scope and Caveats	Approach: Black box with unprivileged physical access
Penetration Testing Team	▮▮▮▮▮▮▮▮▮▮
Organisation	▮▮▮▮▮▮▮▮
Penetration Testing Tools Used	▮▮▮▮▮▮▮▮
Summary of the penetration test performed	Authentication flaws with low, medium and high impact. Session management flaws low, medium and high impact. Input validation flaw with high impact. Cryptography flaw with high impact. Configuration flaws with low, medium and high impact.
Summary of Penetration Testing Findings according to CVSS 3.1	4 findings with high impact 3 findings with medium impact
Prioritized Vulnerabilities Findings	Please see annex 1
Risk and Impact Ranked Findings	Please see annex 1
Follow-up activities	Report handed over to ▮▮▮▮▮▮▮ Fixing activities are pending.
Annex No and name (if relevant)	Annex 1 – Findings and Impact

---

[1] Comprehensive security test – penetration test

Article 35 subsection 1 clause 9 of Public Information Act: https://www.riigiteataja.ee/en/eli/503052023003/consolide; "9) information including a description of security systems, security organisations or security measures;"

Annex 1 – Findings and Impact

CWE ID	Section	Confidentiality Impact	Integrity Impact	Accessibility Impact	CVSS 3.1 Score
494	Download of code without integrity check	Low	Low	Low	4.8 (Medium) Calculation
862	Missing Authorization	High	High	Medium	7.3 (High) Calculation
285	Improper Authorization	Critical	Critical	High	7.8 (High) Calculation
36	Absolute Path Traversal	Low	Low	Low	5.3 (Medium) Calculation
36	Absolute Path Traversal	Low	Low	Low	5.3 (Medium) Calculation
286	Incorrect User Management	High	Medium	Low	7.6 (High) Environmental Score Calculation
286	Incorrect User Management	Crtical	Low	Low	8.8 (High) Environmental Score Score