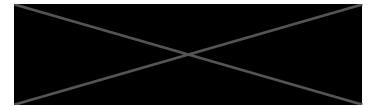




COMPREHENSIVE SECURITY TEST¹ No 21

BACKGROUND INFORMATION²:	
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	25.11.2024 – 19.12.2024
Objective of the Penetration Testing	Detect vulnerabilities in windows active directory and windows infrastructure using Mitre Att&ck framework.
Approach, Scope and Caveats	Approach: Gray box testing with access to documentation.
Penetration Testing Team	
Organisation	
Penetration Testing Tools Used	
Summary of the penetration test performed	1 Credential Access flaw with critical impact. 5 Credential Access flaws with high impact. 4 Credential Access flaw with medium impact. 2 User Account management flaws with medium impact., 1 User Account management flaw with high impact. 2 Active Directory configuration flaws with low impact. 2 Active Directory configuration flaws with medium impact. 1 Software update flaw with high impact. 1 Software update flaw with medium impact. 1 Privileged access management flaw with high impact 1 Privileged access management flaw with medium impact 1 Privileged process integrity flaw with medium impact. 1 Auditing flaw with low impact.
Summary of Penetration Testing Findings according to CVSS 3.1	1 finding with critical impact 8 finding with high impact 11 finding with medium impact 3 finding with low impact 6 finding with informational level

Comprehensive security test – penetration test



Annex 1 – Findings and Impact

Prioritized Findings	Vulnerabilities	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

CWE ID	MITRE Reference	Confidentiality Impact	Integrity Impact	Accessibility Impact	CVSS 3.1 Score
327	T1558.004	High	High	High	9 Critical Calculation
326	T1557.001	High	Medium	Low	7.5 High (Environmental) Calculation
269	M1015	Low	Low	Low	3.9 Low Calculation
269	M1018	Low	Medium	Low	6.3 Medium Calculation
284	M1018	Low	Low	Low	4.6 Medium Calculation
300	T1557.001	Low	High	Low	8.2 High Calculation
841	M1018	High	High	High	8 High Calculation
1104	M1051	Low	High	Low	7.4 High (Temporal) Calculation
521	M1015	Low	None	Low	3.4 Low Calculation
754	M1051	Low	Low	Low	4.3 Medium Calculation
522	T1558.003	Medium	Medium	Low	5.1 Medium Calculation
732	M1015	Medium	Low	Low	5.1 Medium Calculation
521	T1003.004	Low	Low	Low	4.3 Medium Calculation
266	M1015	None	None	None	Info
250	M1026	High	High	High	7.6 High Calculation
269	M1025	Medium	Low	Low	4.6 Medium Calculation
263	M1026	High	Low	High	6.4 Medium Calculation
732	M1015	Medium	Low	Low	5.1 Medium Calculation
276	M1015	None	None	None	Info

Comprehensive security test – penetration test



Annex 1 – Findings and Impact

620	T1558.001	High	High	High	8 High Calculation
778	M1026	None	None	None	Info
778	M1047	Low	Low	None	3.7 Low
276	T1557.001	High	High	High	8.8 High Calculation
347	T1557	Low	Medium	Low	5.1 Medium Calculation
300	T1557	High	High	High	8.1 High Calculation
200	T1555.005	Medium	Medium	Low	5.5 Medium Calculation
266	T1110.003	None	None	None	Info
326	T1600.001	None	None	None	Info
778	M1047	None	None	None	Info