kleosec CYBERSECURITY SERVICES

REMEDIATION REPORT

Remediation Report: invoicing web application

Sample of the report KleoSEC delivers after remediating penetration-test findings. It follows the anonymised report R-2026-003 (12 findings). The measures and evidence are illustrative, the structure and level of detail are real.

> Sample document, anonymised and illustrative. Follows report R-2026-003.

DATE	PREPARED BY	CLASSIFICATION	FINDINGS
28/10/2026	KleoSEC d.o.o.	CONFIDENTIAL	12 addressed

Summary

Of the 12 findings from penetration test R-2026-003, 11 have been remediated and confirmed by retest, and 1 has been partially remediated with a compensating control and the residual risk accepted. Both critical findings (BOLA/IDOR on invoices, MFA configuration takeover) were closed within the first 10 days of remediation.

Status	Findings	IDs
Remediated, confirmed by retest	11	1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12
Partially remediated, residual risk accepted	1	10 (Arbitrary File Upload: validation and proxy in place, antivirus scanning planned)
Open	0	none

Beyond the individual findings, four systemic root causes from the report were addressed: authorisation is now enforced centrally in the data-access layer, authentication issues a token only after all factors, rate limiting and security headers are applied at framework level, and outbound traffic from application servers is restricted. Evidence for every measure is referenced in the findings table and provided in the evidence archive (E-01 to E-14).

Scope and course of remediation

Remediation took six weeks after delivery of the report. Application code changes were made by the client's development team following the remediation plan KleoSEC prepared from the findings. KleoSEC implemented the infrastructure measures (network filtering, storage configuration, security headers), reviewed every code change before production release and confirmed remediation by retest on the production environment.

Item	Detail
Baseline	Report R-2026-003 v1.0, 12 findings (2 critical, 2 high, 7 medium, 1 low)
Environments	Production (11 findings) and development (1 finding)
Division of work	Code: client development team · Infrastructure and configuration: KleoSEC · Review and retest: KleoSEC
Sequence	Weeks 1–2 critical and high · Weeks 3–5 medium and low · Week 6 retest and evidence
Verification method	Repeating the original proof of concept from the report against the remediated environment. A finding is closed only when the PoC no longer succeeds
Evidence archive	E-01 to E-14: retest requests and responses, configuration exports, code-review records, log extracts

Findings and status

#	Finding (severity)	Measure implemented	Evidence	Retest	Status
1	Unauthorized Cross-Tenant Access to Invoice Data, BOLA/IDOR (critical)	Object-level authorisation in the data-access layer: invoice queries scoped to the SME in the JWT, InvoiceID not accepted without an ownership check. Same for PDF generation and the other 6 patterns in the finding	E-01: code review (PR), E-02: retest requests for foreign IDs return 403	PoC fails	Remediated
2	Multi-factor Authentication Takeover (critical)	UserID for OTP enrolment and verification derived from the JWT, not the URL. MFA changes require re-authentication. User notification and audit log entry	E-03: retest, E-04: sample audit entry and e-mail notification	PoC fails	Remediated
3	2FA Bypass (high)	Full JWT issued only after both factors. Short-lived intermediate token valid only for the OTP endpoint	E-05: retest with intermediate token against protected endpoints returns 401	PoC fails	Remediated
4	Blind Server-Side Request Forgery (medium)	PDF renderer without outbound network access, images only from local storage. NSG rules block IMDS, Wire Server and RFC 1918 for application servers	E-06: NSG rule export, E-07: retest with no OAST callback	PoC fails	Remediated
5	Long Session Timeout, JWT (medium)	Access token 15 min + refresh token 24 h, idle timeout 60 min, denylist for revocation on logout and password change	E-08: decoded tokens with new lifetimes, revocation test	Confirmed	Remediated
6	Low Password Complexity Policy (medium)	Server-side policy: min. 8 characters with MFA, max. 64, screening against breached-password database, forced change at next login	E-09: retest with weak passwords (rejected)	Confirmed	Remediated
7	Client-Side Enforcement of Server-Side Security (medium)	API rejects invoice creation and dispatch without mandatory company data, regardless of the UI	E-10: retest by direct API call returns 422	PoC fails	Remediated
8	Clickjacking (medium)	Content-Security-Policy: frame-ancestors 'none' at framework level for all responses	E-11: response header capture	Confirmed	Remediated
9	HTML Injection in Emails (medium)	Freeform HTML template replaced by a structured template with variables. Sender visible in the message body. Audit log of sends	E-12: retest with HTML content (escaped), sample audit entry	PoC fails	Remediated

#	Finding (severity)	Measure implemented	Evidence	Retest	Status
10	Arbitrary File Upload (medium)	Allowlist of types and magic-bytes check. Files served through an authenticated proxy with Content-Disposition: attachment and nosniff. Direct Blob URLs disabled	E-13: retest uploading executables (rejected), direct URL access test (403)	PoC fails	**Partial: antivirus scanning (Defender for Storage) planned for Q1, risk accepted with allowlist and proxy**
11	Password Reset Token Reuse (low)	One-time jti with server-side record, token lifetime 60 min, invalidation of all tokens and sessions after password change	E-14: retest of token reuse (rejected)	PoC fails	**Remediated**
12	Missing Rate Limiter, development environment (high)	Central rate-limiting middleware: 5 failed logins → progressive delay up to 15 min + CAPTCHA, daily e-mail quota per user and organisation, log alerts	E-05 (addendum): retest with 50 login attempts, alert capture	PoC fails	**Remediated**

Systemic measures

Alongside the individual findings, the report named seven systemic root causes. For each, a framework- or infrastructure-level measure was introduced so the same class of finding does not return in the next application release.

Root cause from the report	Measure introduced	Owner
Weak authentication and account protection	Single login flow: token only after all factors. Password policy and breached-password screening in a shared library	Development team
Inconsistent authorisation	Central object-ownership check in the data-access layer. Identity only from the JWT. Unit tests for cross-tenant access in CI	Development team, KleoSEC review
Insecure session and token management	Short access tokens, refresh with idle timeout, denylist for revocation, jti for one-time tokens	Development team
Insufficient server-side input validation	Structured templates instead of freeform HTML. Renderer without network access	Development team, KleoSEC configuration
Insecure upload and storage	Allowlist + magic bytes + authenticated proxy. Defender for Storage planned	KleoSEC, client IT
Overreliance on client-side controls	Rule: every business restriction has a server-side check. Added to the code-review checklist	Development team
Security headers and rate limiting not at framework level	Middleware for CSP, nosniff and rate limiting applied globally. NSG egress rules for application servers	KleoSEC

Mapping to ISO 27001 and NIS2

This table is for the consultant or internal audit: each finding is tied to a control from ISO/IEC 27001:2022 Annex A and a measure from NIS2 Art. 21(2), with the evidence from the archive that can be attached to the documentation.

#	Finding	ISO 27001:2022 Annex A	NIS2 Art. 21(2)	Evidence
1	BOLA/IDOR on invoices	A.5.15 access control, A.8.3 information access restriction, A.8.26 application security requirements	(e), (i)	E-01, E-02
2	MFA configuration takeover	A.8.5 secure authentication, A.8.15 logging	(j)	E-03, E-04
3	2FA Bypass	A.8.5	(j)	E-05
4	Blind SSRF	A.8.26, A.8.20 network security, A.8.9 configuration management	(e)	E-06, E-07
5	Long session lifetime (JWT)	A.8.5	(i), (j)	E-08
6	Weak password policy	A.5.17 authentication information	(i)	E-09
7	Client-side-only enforcement	A.8.26, A.8.29 security testing in development	(e)	E-10
8	Clickjacking	A.8.26, A.8.9	(e)	E-11
9	HTML injection in e-mail	A.8.26, A.8.15	(e)	E-12
10	Arbitrary file upload	A.8.7 protection against malware, A.8.26, A.8.3	(e)	E-13
11	Password reset token reuse	A.8.5, A.5.17	(i)	E-14
12	Missing rate limiter	A.8.5, A.8.16 monitoring activities	(j), (b)	E-05

The penetration test itself and this retest cover A.8.8 (management of technical vulnerabilities) and A.8.29, i.e. NIS2 Art. 21(2)(e) and (f), assessing the effectiveness of measures.

Residual risk and recommendations

The only open risk is the absence of antivirus scanning of uploaded files (finding 10). The type allowlist, content check and serving through an authenticated proxy already prevent the platform from being used to distribute malicious files via public links. The residual risk is that an authenticated user uploads an infected PDF that another user downloads. The client has accepted this risk until Defender for Storage is introduced, planned for Q1.

Recommendations for the next 12 months:

- Introduce Defender for Storage and close finding 10. KleoSEC retests after rollout.
- Repeat the penetration test after the next major application release or within 12 months at the latest (A.8.8, NIS2 Art. 21(2)(f)).
- Keep the cross-tenant unit tests and the code-review checklist in CI as a permanent control.
- Verify rate limiting and security headers on every deployment with an automated test.

Document control

Item	Detail
Reference	R-2026-003-IR, version 1.0
Relates to	Penetration test report R-2026-003 v1.0
Classification	Confidential. This sample is anonymised and illustrative
Prepared by	KleoSEC d.o.o., Mislav Kovač
Recipients	Client management, head of development, compliance consultant
Attachments	Evidence archive E-01 to E-14 (delivered separately, encrypted)