IZVJEŠĆE O PROVEDBI MJERA

Izvješće o provedbi mjera: web aplikacija za fakturiranje

Primjer izvješća koje KleoSEC isporučuje nakon sanacije nalaza iz penetracijskog testa. Nastavlja se na anonimizirani izvještaj R-2026-003 (12 nalaza), provedene mjere i dokazi su ilustrativni, struktura i razina detalja su stvarne.

> Primjer dokumenta, anonimizirano i ilustrativno. Nastavak izvještaja R-2026-003.

DATUM
28.10.2026

IZRADIO
KleoSEC d.o.o.

KLASIFIKACIJA
POVJERLJIVO

NALAZA
12 obrađeno

Sažetak

Od 12 nalaza iz penetracijskog testa R-2026-003, 11 je sanirano i potvrđeno retestom, a 1 je saniran djelomično uz kompenzacijsku mjeru i prihvaćen preostali rizik. Oba kritična nalaza (BOLA/IDOR na računima, preuzimanje MFA konfiguracije) zatvorena su u prvih 10 dana provedbe.

Status	Broj nalaza	Nalazi
Sanirano, retest potvrdio	11	1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12
Djelomično sanirano, preostali rizik prihvaćen	1	10 (Arbitrary File Upload: validacija i proxy uvedeni, antivirusno skeniranje planirano)
Otvoreno	0	nema

Uz pojedinačne nalaze, otklonjena su četiri sistemska uzroka iz izvještaja: autorizacija se sada provodi centralno u sloju pristupa podacima, autentikacija izdaje token tek nakon oba faktora, rate limiting i sigurnosna zaglavlja primjenjuju se na razini okvira, a izlazni mrežni promet aplikacijskih poslužitelja je ograničen. Dokazi za svaku mjeru navedeni su u tablici nalaza i priloženi u arhivi dokaza (E-01 do E-14).

Opseg i tijek provedbe

Provedba je trajala šest tjedana nakon isporuke izvještaja. Izmjene u kodu aplikacije radio je razvojni tim klijenta prema planu provedbe koji je KleoSEC pripremio iz nalaza. KleoSEC je proveo infrastrukturne mjere (mrežni filtri, konfiguracija pohrane, sigurnosna zaglavlja), pregledao svaku izmjenu koda prije puštanja u produkciju i potvrdio sanaciju retestom na produkcijskoj okolini.

Stavka	Detalj
Polazište	Izvještaj R-2026-003 v1.0, 12 nalaza (2 kritična, 2 visoka, 7 srednjih, 1 nizak)
Okoline	Produkcija (11 nalaza) i razvojna okolina (1 nalaz)
Podjela rada	Kod: razvojni tim klijenta · Infrastruktura i konfiguracija: KleoSEC · Pregled i retest: KleoSEC
Redoslijed	Tjedan 1–2 kritični i visoki nalazi · Tjedan 3–5 srednji i niski · Tjedan 6 retest i dokazi
Način verifikacije	Ponavljanje izvornog dokaza (PoC) iz izvještaja na saniranoj okolini. Nalaz je zatvoren tek kad PoC više ne uspijeva
Arhiva dokaza	E-01 do E-14: zahtjevi i odgovori s retesta, izvozi konfiguracija, snimke pregleda koda, zapisi iz dnevnika

Pregled nalaza i statusa

#	Nalaz (ozbiljnost)	Provedena mjera	Dokaz	Retest	Status
1	Unauthorized Cross-Tenant Access to Invoice Data, BOLA/IDOR (kritično)	Autorizacija na razini objekta u sloju pristupa podacima: upiti za račune ograničeni na SME iz JWT-a, InvoiceID se ne prihvaća bez provjere vlasništva. Isto za PDF generiranje i ostalih 6 obrazaca iz nalaza	E-01: pregled koda (PR), E-02: retest zahtjevi za tuđe ID-ove vraćaju 403	PoC ne uspijeva	Sanirano
2	Multi-factor Authentication Takeover (kritično)	UserID za OTP upis i verifikaciju izveden iz JWT-a, ne iz URL-a. Promjena MFA traži ponovnu autentikaciju. Obavijest korisniku i zapis u audit log	E-03: retest, E-04: primjer audit zapisa i e-mail obavijesti	PoC ne uspijeva	Sanirano
3	2FA Bypass (visoko)	Puni JWT izdaje se tek nakon oba faktora. Međutoken kratkog vijeka vrijedi samo za OTP endpoint	E-05: retest s međutokenom na zaštićene endpointe vraća 401	PoC ne uspijeva	Sanirano
4	Blind Server-Side Request Forgery (srednje)	PDF renderer bez izlaznog mrežnog pristupa, slike samo iz lokalne pohrane. NSG pravila blokiraju IMDS, Wire Server i RFC 1918 za aplikacijske poslužitelje	E-06: izvoz NSG pravila, E-07: retest bez OAST callbacka	PoC ne uspijeva	Sanirano
5	Long Session Timeout, JWT (srednje)	Access token 15 min + refresh token 24 h, idle timeout 60 min, denylist za opoziv pri odjavi i promjeni lozinke	E-08: dekodirani tokeni s novim vijekom, test opoziva	Potvrđeno	Sanirano
6	Low Password Complexity Policy (srednje)	Server-side politika: min. 8 znakova uz MFA, max. 64, provjera prema bazi kompromitiranih lozinki, prisilna promjena pri sljedećoj prijavi	E-09: retest sa slabim lozinkama (odbijene)	Potvrđeno	Sanirano
7	Client-Side Enforcement of Server-Side Security (srednje)	API odbija izradu i slanje računa bez obveznih podataka o tvrtki, neovisno o sučelju	E-10: retest direktnim API pozivom vraća 422	PoC ne uspijeva	Sanirano
8	Clickjacking (srednje)	Content-Security-Policy: frame-ancestors 'none' na razini okvira za sve odgovore	E-11: snimka zaglavlja odgovora	Potvrđeno	Sanirano
9	HTML Injection in Emails (srednje)	Slobodni HTML predložak zamijenjen strukturiranim predloškom s varijablama. Pošiljatelj vidljiv u tijelu poruke. Audit log slanja	E-12: retest s HTML sadržajem (escapiran), primjer audit zapisa	PoC ne uspijeva	Sanirano

#	Nalaz (ozbiljnost)	Provedena mjera	Dokaz	Retest	Status
10	Arbitrary File Upload (srednje)	Allowlist tipova i provjera magic bytes. Datoteke se poslužuju kroz autenticirani proxy s Content-Disposition: attachment i nosniff. Direktni Blob URL-ovi ugašeni	E-13: retest uploada izvršnih datoteka (odbijen), test pristupa direktnom URL-u (403)	PoC ne uspijeva	Djelomično: antivirusno skeniranje (Defender for Storage) planirano za Q1, rizik prihvaćen uz allowlist i proxy
11	Password Reset Token Reuse (nisko)	Jednokratni jti s server-side evidencijom, vijek tokena 60 min, poništenje svih tokena i sesija nakon promjene lozinke	E-14: retest ponovne upotrebe tokena (odbijen)	PoC ne uspijeva	Sanirano
12	Missing Rate Limiter, razvojna okolina (visoko)	Centralni rate-limiting middleware: 5 neuspjelih prijava → progresivna odgoda do 15 min + CAPTCHA, dnevna kvota slanja e-pošte po korisniku i organizaciji, alarmi u dnevniku	E-05 (dopuna): retest 50 pokušaja prijave, snimka alarma	PoC ne uspijeva	Sanirano

Sistemske mjere

Izvještaj je uz pojedinačne nalaze imenovao sedam sistemskih uzroka. Za svaki je uvedena mjera na razini okvira ili infrastrukture, tako da se isti tip nalaza ne vraća u sljedećoj verziji aplikacije.

Sistemski uzrok iz izvještaja	Uvedena mjera	Vlasnik
Slaba autentikacija i zaštita računa	Jedinstveni tijek prijave: token tek nakon svih faktora. Politika lozinki i provjera kompromitiranih lozinki u zajedničkoj biblioteci	Razvojni tim
Nedosljedna autorizacija	Centralna provjera vlasništva objekta u sloju pristupa podacima. Identitet isključivo iz JWT-a. Unit testovi za cross-tenant pristup u CI-ju	Razvojni tim, KleoSEC pregled
Nesigurno upravljanje sesijama i tokenima	Kratki access tokeni, refresh s idle timeoutom, denylist za opoziv, jti za jednokratne tokene	Razvojni tim
Nedovoljna validacija ulaza na poslužitelju	Strukturirani predlošci umjesto slobodnog HTML-a. Renderer bez mrežnog pristupa	Razvojni tim, KleoSEC konfiguracija
Nesiguran upload i pohrana	Allowlist + magic bytes + autenticirani proxy. Defender for Storage u planu	KleoSEC, klijentov IT
Oslanjanje na klijentsku stranu	Pravilo: svaka poslovna restrikcija ima server-side provjeru. Dodano u checklistu pregleda koda	Razvojni tim
Sigurnosna zaglavlja i rate limiting nisu na razini okvira	Middleware za CSP, nosniff i rate limiting primijenjen globalno. NSG egress pravila za aplikacijske poslužitelje	KleoSEC

Mapiranje na ISO 27001 i NIS2

Tablica je namijenjena konzultantu ili internom auditu: svaki nalaz vezan je uz kontrolu iz ISO/IEC 27001:2022 Annex A i mjeru iz NIS2 čl. 21(2), uz dokaz iz arhive koji se može priložiti dokumentaciji.

#	Nalaz	ISO 27001:2022 Annex A	NIS2 čl. 21(2)	Dokaz
1	BOLA/IDOR na računima	A.5.15 kontrola pristupa, A.8.3 ograničenje pristupa informacijama, A.8.26 sigurnosni zahtjevi aplikacija	(e), (i)	E-01, E-02
2	Preuzimanje MFA konfiguracije	A.8.5 sigurna autentikacija, A.8.15 zapisivanje	(j)	E-03, E-04
3	2FA Bypass	A.8.5	(j)	E-05
4	Blind SSRF	A.8.26, A.8.20 mrežna sigurnost, A.8.9 upravljanje konfiguracijom	(e)	E-06, E-07
5	Dug vijek sesije (JWT)	A.8.5	(i), (j)	E-08
6	Slaba politika lozinki	A.5.17 informacije za autentikaciju	(i)	E-09
7	Provjera samo na klijentskoj strani	A.8.26, A.8.29 sigurnosno testiranje u razvoju	(e)	E-10
8	Clickjacking	A.8.26, A.8.9	(e)	E-11
9	HTML injection u e-pošti	A.8.26, A.8.15	(e)	E-12
10	Proizvoljan upload datoteka	A.8.7 zaštita od malwarea, A.8.26, A.8.3	(e)	E-13
11	Ponovna upotreba tokena za reset lozinke	A.8.5, A.5.17	(i)	E-14
12	Nedostaje rate limiter	A.8.5, A.8.16 nadzor aktivnosti	(j), (b)	E-05

Sam penetracijski test i ovaj retest pokrivaju A.8.8 (upravljanje tehničkim ranjivostima) i A.8.29, odnosno NIS2 čl. 21(2)(e) i (f), procjenu učinkovitosti mjera.

Preostali rizik i preporuke

Jedini otvoreni rizik je izostanak antivirusnog skeniranja datoteka na uploadu (nalaz 10). Allowlist tipova, provjera sadržaja i posluživanje kroz autenticirani proxy već onemogućuju korištenje platforme za distribuciju zlonamjernih datoteka javnim linkom. Preostali rizik je da autenticirani korisnik učita zaraženi PDF koji drugi korisnik preuzme. Klijent je rizik prihvatio do uvođenja Defender for Storage, planiranog za Q1.

Preporuke za sljedećih 12 mjeseci:

- Uvesti Defender for Storage i zatvoriti nalaz 10. KleoSEC radi retest nakon uvođenja.

- Ponoviti penetracijski test nakon sljedeće veće verzije aplikacije ili najkasnije za 12 mjeseci (A.8.8, NIS2 čl. 21(2)(f)).
- Zadržati unit testove za cross-tenant pristup i checklistu pregleda koda u CI-ju kao trajnu kontrolu.
- Rate-limiting i sigurnosna zaglavlja provjeravati pri svakom deployu automatiziranim testom.

Kontrola dokumenta

Stavka	Detalj
Oznaka	R-2026-003-IR, verzija 1.0
Odnosi se na	Izvještaj o penetracijskom testu R-2026-003 v1.0
Klasifikacija	Povjerljivo. Ovaj primjer je anonimiziran i ilustrativan
Izradio	KleoSEC d.o.o., Mislav Kovač
Primatelji	Uprava klijenta, voditelj razvoja, konzultant za usklađenost
Prilozi	Arhiva dokaza E-01 do E-14 (dostavlja se odvojeno, šifrirano)