BEZPEČNOSTNÝ AUDIT

Technický report

NovaSoft s.r.o. — účtovný a mzdový systém NovaPay

KLIENT NovaSoft s.r.o.	OBDOBIE 1.–12. apr 2026	DÁTUM SPRÁVY 15. apr 2026
AUDÍTOR Security s.r.o.	NÁLEZY 7 (1C 2H 2M 2I)	ZÁVAŽNOSŤ Kritická

DÔVERNÉ

OBSAH

Štruktúra dokumentu

DISTRIBÚCIA

Určenie dokumentu

Tento dokument je určený výhradne pre technický tím klienta zodpovedný za opravu identifikovaných zraniteľností. Obsahuje reprodukčné kroky, zdrojový kód, konfigurácie a ďalšie technické detaily, ktoré by v rukách neoprávnenej osoby umožnili zneužitie popísaných zraniteľností. **Nekopírujte a nezdieľajte tento dokument mimo dohodnutého okruhu príjemcov.**

Paralelne bol klientovi doručený dokument **Správa pre vedenie**, ktorý obsahuje netechnické zhrnutie nálezov, biznis dopad a odporúčané priority. Je určený pre manažment a neobsahuje reprodukčné detaily.

01 — ROZSAH A METODOLÓGIA

Testované aktíva

AKTÍVUM	TYP	VERZIA / BUILD
`app.novasoft.sk`	Webová aplikácia (React 18 + ASP.NET Core 6)	Build 4.2.1-rc3
`api.novasoft.sk`	REST API (.NET 6, Swagger/OpenAPI 3.0)	v2.8.0
`cz.novasoft.novapay`	Android APK (Kotlin, minSdk 26)	v4.2.1 (versionCode 89)
`admin.novasoft.sk`	Administrátorský portál (React + ASP.NET)	Build 2.1.4
`*.novasoft.sk`	Subdomény (38 identifikovaných, 22 live)	—

Metodológia

Externý bezpečnostný audit podľa OWASP Testing Guide v4.2 a PTES (Penetration Testing Execution Standard). Tri fázy: (1) automatizované skenovanie povrchu a závislostí (nuclei, semgrep, osv-scanner, trufflehog), (2) statická analýza decompilovaného kódu (ilspycmd pre .NET, jadx pre Android), (3) manuálne testovanie a verifikácia nálezov. Všetky testy boli vykonané z externého prostredia cez komerčnú VPN (Mullvad, WireGuard). Žiadne testy z internej siete klienta.

Obmedzenia

Audit nepokrýva internú sieť, fyzickú bezpečnosť, sociálne inžinierstvo, ani systémy tretích strán (Azure control plane, platobná brána, CDN). Deštruktívne testovanie a hromadná extrakcia dát neboli vykonávané. Tam kde je exploit deštruktívny, je to v reporte výslovne uvedené a závažnosť je primerane upravená.

Klasifikácia závažnosti

ÚROVEŇ	DEFINÍCIA	OPRAVA
KRITICKÝ	Existenčné ohrozenie — masívny únik dát, plný kompromis infraštruktúry, supply chain	Okamžite (do 48 h)
VYSOKÝ	Vážna škoda — obmedzený únik dát, admin kompromis, auth bypass	Do 7 dní
STREDNÝ	Významná expozícia — cross-customer viditeľnosť, XSS, insider abuse potenciál	Najbližší release
INFO	Hygienické pozorovanie — chýbajúce hlavičky, verbose chyby, zastarané knižnice bez exploitu	Maintenance cyklus

02 — SÚHRN INFRAŠTRUKTÚRY

Architektúra NovaPay z pohľadu útočníka

Počas rekognoskácie sme identifikovali nasledujúcu externú infraštruktúru:

KOMPONENT	TECHNOLÓGIA	POZNÁMKA
Frontend	React 18 za Cloudflare CDN	SPA, SSR nie
API backend	ASP.NET Core 6, Kestrel za nginx reverse proxy	Swagger UI prístupný na `/swagger`
Databáza	PostgreSQL 14 (inferované z Npgsql v stack trace)	Externe neprístupná
Úložisko	Azure Blob Storage (`novasoftprod`)	Kľúč v APK (F-03)
Mobile app	Kotlin, OkHttp 4.12, cert pinning chýba	Google Play distribúcia
Admin portál	React + ASP.NET, rovnaký API backend	Externe prístupný (F-04)
E-mail	SMTP cez SendGrid (API key v app config)	Transakčné maily
Auth	JWT RS256, refresh tokeny, žiadne MFA	Rate limit chýba (F-05)

Identifikované subdomény

Z 38 identifikovaných subdomén (`crt.sh` + `subfinder`) bolo 22 živých. Okrem primárnych aktív (viď sekcia 01) sme identifikovali:

SUBDOMÉNA	STAV	POZNÁMKA
`staging.novasoft.sk`	200 OK	Staging prostredie s produkčnou DB (rovnaké dáta ako prod!)
`grafana.novasoft.sk`	302 → login	Grafana 10.2.1, default admin login netestovaný
`jenkins.novasoft.sk`	403	Jenkins za IP whitelistom
`docs.novasoft.sk`	200 OK	Interná API dokumentácia, verejne prístupná
`legacy-api.novasoft.sk`	200 OK	Staršia API verzia (v1), stále aktívna, rovnaká DB
`mail.novasoft.sk`	443 timeout	MX záznam, SMTP

Pozoruhodné: `staging.novasoft.sk` zdieľa produkčnú databázu. Všetky nálezy API (F-01, F-02, F-05) sú reprodukovateľné aj na staging endpointe. Staging nemá Cloudflare ochranu, čo znižuje bariéru pre útočníka.

03 — NÁLEZ F-01

IDOR — neoprávnený prístup k zákazníckym mzdovým dátam

F-01 KRITICKÝ **Broken Access Control na payroll API endpointoch**

CWE	OWASP	AKTÍVUM	OVERENIE
CWE-862	A01:2021	`api.novasoft.sk`	Reprodukované (live)

POPIS ZRANITEĽNOSTI

Endpoint `/api/v2/payroll/employees/{companyId}` akceptuje parameter `companyId` priamo z URL path-u, ale **neoveruje, či prihlásený používateľ patrí k požadovanej spoločnosti**. Parameter je sekvenčné celé číslo v rozsahu 1 – ~4 200. Útočník s bežným trial účtom (registrácia trvá 30 sekúnd) získa prístup k mzdovým záznamom ľubovoľnej spoločnosti v systéme.

Rovnaký vzorec chýbajúcej autorizácie sme identifikovali na ďalších **14 endpointoch** v `/api/v2/payroll/*` namespace-i vrátane `/payslips`, `/tax-returns`, `/social-insurance` a `/bank-accounts`.

REPRODUKČNÉ KROKY

1. Registrácia trial účtu na `app.novasoft.sk/register` (e-mail + heslo)
2. Prihlásenie cez `POST /api/v2/auth/login` → Bearer JWT token
3. Odoslanie requestu s cudzím `companyId`:

```
GET /api/v2/payroll/employees/12345 HTTP/1.1
Host: api.novasoft.sk
Authorization: Bearer eyJhbGciOiJSUzI1NiIs...skrátené
Accept: application/json
```

ODPOVEĎ SERVERA (REDAKTOVANÉ PII)

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-Id: 7f3a2b1c-4d5e-6f7a-8b9c-0d1e2f3a4b5c

{
  "companyId": 12345,
  "companyName": "[redacted] s.r.o.",
  "ico": "[redacted]",
  "employees": [
    {
      "employeeId": 89234,
      "firstName": "[redacted]",
      "lastName": "[redacted]",
      "birthNumber": "[redacted]/[redacted]",
      "personalIdNumber": "[redacted]",
      "bankAccount": "SK[redacted]",
      "address": "[redacted], [redacted]",
      "grossSalary": [redacted],
      "netSalary": [redacted],
      "taxBase": [redacted],
      "healthInsurance": [redacted],
      "socialInsurance": [redacted]
    }
    // ... ďalší zamestnanci
  ],
  "totalEmployees": 47,
  "generatedAt": "2026-04-08T14:22:31Z"
}
```

DÔKAZ

Overené na 3 náhodných `companyId` hodnotách (12345, 12346, 12400). Každý vrátil kompletné mzdové záznamy inej spoločnosti. Extrahované iba prvé 2 záznamy z každej odpovede — hromadná extrakcia nevykonaná.

SHA-256 response body (companyId=12345):

`e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`

Dotknuté endpointy (rovnaký vzorec):

`/api/v2/payroll/employees/{id}`, `/payslips/{id}`, `/tax-returns/{id}`, `/social-insurance/{id}`, `/bank-accounts/{id}`, `/attendance/{id}`, `/contracts/{id}`, `/bonuses/{id}`, `/deductions/{id}`, `/departments/{id}`, `/positions/{id}`, `/salary-history/{id}`, `/documents/{id}`, `/exports/{id}`, `/reports/{id}`

DOPAD

Pri ~4 200 aktívnych spoločnostiach a priemerne ~20 zamestnancoch na spoločnosť je exponovaných **~85 000 kompletných mzdových záznamov** vrátane: meno, rodné číslo, číslo OP, adresa, bankový účet, výška platu, daňové podklady, zdravotné a sociálne odvody, pracovné zmluvy.

Údaje spadajú pod GDPR čl. 9 (osobitná kategória) a zákon č. 18/2018 Z.z. Regulátor (ÚOOÚ) je oprávnený uložiť sankciu až do výšky 4 % ročného obratu.

ODPORÚČANIE NA OPRAVU

Implementovať autorizačnú kontrolu na úrovni middleware alebo controllera. Každý request musí overiť, že `companyId` zodpovedá spoločnosti priradenej autentifikovanému používateľovi:

```
// PayrollController.cs — pridať na všetkých 15 endpointoch
[Authorize]
public async Task<IActionResult> GetEmployees(int companyId)
{
    var userCompanyId = User.Claims
        .First(c ⇒ c.Type == "company_id").Value;
    if (companyId.ToString() ≠ userCompanyId)
        return Forbid();

    // ... pôvodná logika
}
```

Alternatíva (lepšia dlhodobo): Globálny authorization filter na úrovni `/api/v2/payroll/*` route group, ktorý automaticky extrahuje `companyId` z path-u a porovná s claimom v JWT. Eliminuje riziko zabudnutej kontroly na novom endpointe.

04 — NÁLEZ F-02

Vzdialené spustenie kódu cez deserializáciu

F-02 ● VYSOKÝ **RCE cez Newtonsoft.Json TypeNameHandling.Auto**

CWE	ADVISORY	AKTÍVUM	OVERENIE
CWE-502	GHSA-5crp-9r3c-p9vr	`api.novasoft.sk`	Statická analýza kódu

POPIS

Decompilovaný kód API servera (ilspycmd → C#) obsahuje globálnu konfiguráciu JSON deserializácie s nastavením `TypeNameHandling.Auto` v knižnici Newtonsoft.Json 12.0.3. Toto nastavenie umožňuje útočníkovi vložiť do tela JSON požiadavky referenciu na ľubovoľný .NET typ — vrátane typov ako `System.Diagnostics.Process`, `System.IO.File` a gadget chainov pre vzdialené spustenie kódu.

```
// NovaPay.Api.Startup.cs (decompiled, line 147)
services.AddControllers()
    .AddNewtonsoftJson(options ⇒
    {
        options.SerializerSettings.TypeNameHandling =
            TypeNameHandling.Auto;  // ← zraniteľné nastavenie
        options.SerializerSettings.NullValueHandling =
            NullValueHandling.Ignore;
    });
```

EXPLOIT SCENÁR

Útočník identifikuje API endpoint akceptujúci polymorfný JSON objekt (napr. `POST /api/v2/payroll/import` s obecným `object` parametrom) a odošle payload obsahujúci gadget chain:

```
{
  "$type": "System.Windows.Data.ObjectDataProvider, PresentationFramework",
  "MethodName": "Start",
  "MethodParameters": {
    "$type": "System.Collections.ArrayList",
    "$values": ["cmd", "/c calc.exe"]
  },
  "ObjectInstance": {
    "$type": "System.Diagnostics.Process, System"
  }
}
```

Demonštrácia obmedzená rozsahom auditu — odoslanie exploit payloadu by spôsobilo spustenie kódu na produkčnom serveri. Zraniteľnosť je potvrdená statickou analýzou kódu + presnou zhodou verzie s publikovaným advisory.

DOPAD

Vzdialené spustenie ľubovoľného kódu na aplikačnom serveri v kontexte servisného účtu. Ďalej: prístup k PostgreSQL databáze (connection string v `appsettings.json`), Azure Storage kľúčom, SendGrid API kľúču, a sieťovým zdrojom dostupným z aplikačného servera.

ODPORÚČANIE NA OPRAVU

Zmeniť globálne nastavenie na bezpečnú hodnotu:

```
options.SerializerSettings.TypeNameHandling =
    TypeNameHandling.None;  // bezpečné — predvolená hodnota
```

Ak polymorfná deserializácia je nutná pre konkrétne endpointy (napr. import), implementovať vlastný `ISerializationBinder` s explicitným whitelistom povolených typov. Nikdy nepoužívať `Auto` alebo `All` na endpointoch prijímajúcich externý vstup.

Zvážiť migráciu z Newtonsoft.Json na `System.Text.Json` (natívny .NET), ktorý nemá ekvivalent `TypeNameHandling` a je bezpečný v predvolenom nastavení.

05 — NÁLEZ F-03

Hardcoded Azure Storage master key

F-03 VYSOKÝ **Azure Storage Account key v plaintext v mobilnej aplikácii**

CWE	OWASP	AKTÍVUM	OVERENIE
CWE-798	A07:2021	APK `cz.novasoft.novapay`	Reprodukované (read-only)

POPIS

Decompilovaný kód mobilnej aplikácie (jadx) obsahuje prístupový kľúč k Azure Blob Storage v plaintext konštante. Kľúč je **master key** — poskytuje plný prístup (čítanie, zápis, mazanie) ku všetkým kontajnerom v storage účte.

```
// sk/novasoft/novapay/config/CloudConfig.java (jadx output)
public static final String STORAGE_ACCOUNT = "novasoftprod";
public static final String STORAGE_KEY =
    "[redacted]";
public static final String CONTAINER = "customer-exports";
```

REPRODUKČNÉ KROKY

1. Stiahnuť APK z Google Play alebo APKPure
2. Dekomprilovať: `jadx -d output/ cz.novasoft.novapay.apk`
3. Nájsť kľúč: `grep -r "STORAGE_KEY" output/`
4. Overiť prístup (read-only, žiadne dáta stiahnuté):

```
$ az storage container list \
    --account-name novasoftprod \
    --account-key "[redacted]" \
    --output table

Name              Lease Status    Last Modified
----------------  --------------  -------------------------
customer-exports  unlocked        2026-04-07T09:14:22+00:00
payroll-backups   unlocked        2026-04-06T02:00:15+00:00
documents         unlocked        2026-04-08T11:33:47+00:00
temp-imports      unlocked        2026-04-08T14:22:01+00:00
```

DÔKAZ

Kľúč overený `az storage container list` — vrátené 4 kontajnery. Kontajner `payroll-backups` podľa názvu obsahuje zálohy mzdových dát. Žiadne dáta neboli stiahnuté ani modifikované.

DOPAD

Ktokoľvek s prístupom k APK (verejne dostupné na Google Play) môže extrahovať kľúč a získať plný prístup k storage účtu vrátane potenciálnych záloh databázy a zákazníckych exportov. Kľúč je zdieľaný naprieč všetkými inštaláciami aplikácie.

ODPORÚČANIE NA OPRAVU

1. **Okamžite:** Rotovať oba kľúče účtu `novasoftprod` (primárny + sekundárny)
2. **Okamžite:** Skontrolovať Azure Storage Analytics log za posledných 90 dní pre neštandardné prístupy
3. **Krátkodobo:** Nahradiť hardcoded kľúč za server-generated SAS tokeny s obmedzeným scopom a platnosťou (max 1 hodina)
4. **Dlhodobo:** Implementovať Azure Managed Identity alebo Azure AD RBAC — eliminuje statické kľúče úplne

06 — NÁLEZ F-04

Admin rozhranie prístupné z internetu

F-04 STREDNÝ **Administrátorský portál bez sieťového obmedzenia**

CWE	OWASP	AKTÍVUM	OVERENIE
CWE-749	A05:2021	`admin.novasoft.sk`	Potvrdené

POPIS

Administrátorský portál na `admin.novasoft.sk` je dostupný z ľubovoľnej IP adresy bez VPN, IP whitelistu alebo iného sieťového obmedzenia. Login formulár je verejne prístupný. V kombinácii s nálezom F-05 (chýbajúci rate limiting) útočník môže automatizovane skúšať heslá admin účtov.

DOPAD

Úspešné prihlásenie by poskytlo prístup k správe zákazníkov, licencií, systémových nastavení a používateľských účtov. Admin portál používa rovnaký API backend — admin JWT token má scope `admin:*` oproti bežnému `user:read`.

> **ODPORÚČANIE NA OPRAVU**
>
> Obmedziť prístup k `admin.novasoft.sk` na firemný VPN alebo definovaný rozsah IP adries na úrovni nginx / Cloudflare Access. Ako alternatívu implementovať mTLS s klientskym certifikátom. Doplniť MFA (TOTP alebo WebAuthn) na admin login.

07 — NÁLEZ F-05

Chýbajúci rate limiting na prihlásenie

F-05 STREDNÝ **Neobmedzený počet pokusov o prihlásenie**

CWE	OWASP	AKTÍVUM	OVERENIE
CWE-307	A07:2021	`api.novasoft.sk`	Reprodukované

POPIS

Endpoint `POST /api/v2/auth/login` neimplementuje žiadny mechanizmus obmedzenia rýchlosti ani počtu neúspešných pokusov. Odoslanie 50 nesprávnych hesiel z jednej IP adresy za 10 sekúnd nevyvolalo žiadne blokovanie, CAPTCHA ani oneskorenie odpovede.

```
# 50 pokusov, priemerná odozva 84ms, žiadna 429
$ for i in $(seq 1 50); do
    curl -s -o /dev/null -w "%{http_code} %{time_total}s\n" \
      -X POST https://api.novasoft.sk/api/v2/auth/login \
      -H "Content-Type: application/json" \
      -d "{\"email\":\"admin@novasoft.sk\",\"password\":\"guess$i\"}"
  done | head -5

401 0.084s
401 0.079s
401 0.091s
401 0.082s
401 0.088s
... (všetkých 50 rovnako, žiadna 429)
```

ODPORÚČANIE NA OPRAVU

Implementovať rate limiting na `/api/v2/auth/login`: max 5 neúspešných pokusov za 15 minút na kombináciu IP + email. Po 3. neúspešnom pokuse zobraziť CAPTCHA. Po 10. pokuse dočasne zablokovať účet (30 min). Vrátiť `429 Too Many Requests` s hlavičkou `Retry-After`.

08 — NÁLEZ F-06

Zastarané závislosti

F-06 ● INFO **Knižnice s publikovanými bezpečnostnými advisory**

Statická analýza (osv-scanner na decompilovaných assembly referenciách) identifikovala 4 knižnice s vydanými bezpečnostnými opravami. Pre žiadnu z nich sme neidentifikovali priamo zneužiteľnú cestu v kontexte NovaPay — zaradené ako informatívne pozorovanie.

KNIŽNICA	NÁJDENÁ VERZIA	OPRAVENÁ VERZIA	ADVISORY
`System.Text.Json`	6.0.0	8.0.5+	GHSA-hh2w-p6rv-4g7w
`BouncyCastle`	1.8.9	2.4.0+	CVE-2024-29857
`Npgsql`	6.0.4	8.0.6+	CVE-2024-32655
`jQuery`	3.5.1	3.7.1+	CVE-2020-23064

ODPORÚČANIE

Aktualizovať na opravené verzie v rámci najbližšieho maintenance cyklu. Zaviesť automatické skenovanie závislostí (napr. `dotnet list package --vulnerable` v CI pipeline).

09 — NÁLEZ F-07

Chýbajúce HTTP bezpečnostné hlavičky

F-07 ● INFO **Webový portál neodosiela odporúčané security headers**

Odpovede z `app.novasoft.sk` neobsahujú nasledujúce bezpečnostné hlavičky odporúčané OWASP Secure Headers Project:

HLAVIČKA	STAV	ODPORÚČANÁ HODNOTA
`Content-Security-Policy`	Chýba	`default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'`
`Strict-Transport-Security`	Chýba	`max-age=31536000; includeSubDomains; preload`
`X-Content-Type-Options`	Chýba	`nosniff`
`Permissions-Policy`	Chýba	`camera=(), microphone=(), geolocation=()`

HLAVIČKA	STAV	ODPORÚČANÁ HODNOTA
`Referrer-Policy`	Chýba	`strict-origin-when-cross-origin`

ODPORÚČANIE

Pridať hlavičky na úrovni nginx reverse proxy alebo ASP.NET middleware. Príklad pre nginx:

```
# /etc/nginx/conf.d/security-headers.conf
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
add_header X-Content-Type-Options "nosniff" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
add_header Permissions-Policy "camera=(), microphone=(), geolocation=()" always;
```

10 — SUMÁR

Matica nálezov a odporúčané poradie opráv

#	ZÁVAŽNOSŤ	NÁLEZ	CWE	AKTÍVUM	OPRAVA
F-01	KRITICKÝ	IDOR na payroll API — prístup k 85k mzdových záznamov	862	API	Okamžite
F-02	VYSOKÝ	RCE cez Newtonsoft.Json deserialization	502	API	Release
F-03	VYSOKÝ	Hardcoded Azure Storage master key v APK	798	APK	7 dní
F-04	STREDNÝ	Admin portál verejne prístupný	749	Web	Release
F-05	STREDNÝ	Žiadny rate limiting na login	307	API	Release
F-06	INFO	Zastarané knižnice (4×)	—	API	Maintenance
F-07	INFO	Chýbajúce security headers (5×)	—	Web	Maintenance

Bezplatné opakované overenie

Súčasťou zákazky je bezplatné opakované overenie všetkých fakturovateľných nálezov (F-01 až F-05) do 60 dní od doručenia tejto správy, maximálne 3 overenia na jeden nález. Po implementácii opráv nás kontaktujte a dohodneme termín re-testu.

Obmedzenie rozsahu a platnosti. Tento report opisuje nálezy z auditu vykonaného v období 1.–12. apríla 2026 na aktívach definovaných v sekcii 01. Audit je bodové overenie — odzrkadľuje stav systémov v čase vykonania. Neskoršie zmeny systémov môžu priniesť nové zraniteľnosti. Metodológia pokrýva najčastejšie triedy zraniteľností, ale nie je vyčerpávajúca. Neidentifikované zraniteľnosti môžu v systémoch existovať. Tento report nepredstavuje certifikáciu bezpečnosti. Odporúčame pravidelné opakovanie auditu po významných zmenách alebo ročne.