BEZPEČNOSTNÝ AUDIT

# Správa pre vedenie

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

| KLIENT | OBDOBIE AUDITU | AUDÍTOR | DÁTUM SPRÁVY |
| --- | --- | --- | --- |
| NovaSoft s.r.o. | 1. – 12. apr 2026 | Security s.r.o. | 15. apríl 2026 |

— 01 — CELKOVÝ VERDIKT

# Identifikované kritické ohrozenie

KRITICKÁ ZÁVAŽNOSŤ

Identifikovali sme zraniteľnosť, ktorá umožňuje neoprávnenému útočníkovi z internetu získať prístup k mzdovým a osobným údajom všetkých zákazníkov systému NovaPay — vrátane rodných čísiel, výplatných pások a bankových účtov.

Počas 12-dňového auditu sme identifikovali **7 bezpečnostných nálezov**, z toho 1 kritickej, 2 vysokej, 2 strednej a 2 informatívnej závažnosti.

| 1 | 2 | 2 | 2 |
|---|---|---|---|
| KRITICKÝ | VYSOKÉ | STREDNÉ | INFORMATÍVNE |

— 02 — BIZNIS DOPAD

# Čo to znamená pre vašu firmu

Najzávažnejší nález sa týka spôsobu, akým systém NovaPay overuje prístup k programovému rozhraniu. Útočník dokáže pomocou voľne dostupných nástrojov a bez prihlasovacích údajov:

### Únik osobných údajov

Prístup k menám, rodným číslam, adresám a bankovým účtom. Rozsah: **~85 000 zamestnancov** naprieč všetkými zákazníkmi.

### Únik mzdových údajov

Kompletné výplatné pásky, mzdové zložky, odvody a daňové podklady. GDPR čl. 9, zákon č. 18/2018 Z.z.

### Regulačné dôsledky

Sankcia ÚOOÚ až **4 % ročného obratu** podľa GDPR čl. 83. Povinné oznamovanie dotknutým osobám.

### Reputačné riziko

Zákazníci NovaPay zveria systému najcitlivejšie údaje zamestnancov. Verejný únik = strata dôvery a odchod klientov.

— 03 — PREHĽAD NÁLEZOV

# Zoznam identifikovaných problémov

| | | | |
|---|---|---|---|
| F-01 | KRITICKÝ | Neoprávnený prístup k údajom všetkých zákazníkov cez API bez prihlásenia | POTVRDENÝ |
| F-02 | VYSOKÝ | Zastaraná knižnica umožňujúca vzdialené spustenie kódu na serveri | POTVRDENÝ |
| F-03 | VYSOKÝ | Prístupové údaje k cloudovému úložisku vložené priamo do aplikácie | POTVRDENÝ |
| F-04 | STREDNÝ | Administrátorské rozhranie prístupné z internetu bez ďalšej ochrany | POTVRDENÝ |
| F-05 | STREDNÝ | Chýbajúce obmedzenie počtu pokusov o prihlásenie | POTVRDENÝ |
| F-06 | INFO | Zastarané verzie pomocných knižníc bez známeho zneužitia | POZOROVANIE |
| F-07 | INFO | Chýbajúce bezpečnostné hlavičky na webovom portáli | POZOROVANIE |

Podrobný technický popis vrátane reprodukčných krokov nájdete v **Technickom reporte** určenom pre vývojový tím.

— 04 — PORADIE OPRÁV

# Odporúčané priority

1. **F-01 — Neoprávnený prístup k API**
   Nasadiť autorizačnú kontrolu. Odhad: 1–2 pracovné dni.
   DO 48 HODÍN

2. **F-03 — Prístupové údaje v aplikácii**
   Rotovať kľúče, presunúť do Key Vault. Audit log 90 dní.
   DO 7 DNÍ

3. **F-02 — Zastaraná šifrovacia knižnica**
   Aktualizovať na opravenú verziu. Regression testing.
   NAJBLIŽŠÍ RELEASE

4

**F-04 + F-05 — Admin panel a rate limiting**

VPN/IP whitelist + max 5 pokusov za 15 min.

NAJBLIŽŠÍ RELEASE

— 05 — ROZSAH

# Čo bolo testované

| PARAMETER | HODNOTA |
|---|---|
| **Aktíva** | Webový portál (app.novasoft.sk), REST API (api.novasoft.sk), mobilná aplikácia Android (v4.2.1), 38 subdomén |
| **Metodológia** | OWASP Testing Guide v4.2, PTES — automatizované skenovanie, statická analýza, manuálne testovanie |
| **Obmedzenia** | Nepokrýva internú sieť, fyzickú bezpečnosť, sociálne inžinierstvo ani systémy tretích strán. Bez deštruktívneho testovania. |

— 06 — ĎALŠIE KROKY

# Harmonogram

| # | KROK | TERMÍN |
|---|---|---|
| 1 | Záverečná konzultácia (1 hodina, vzdialene) | Do 5 prac. dní |
| 2 | Oprava kritického nálezu F-01 | Do 48 hodín |
| 3 | Lehota na námietky voči závažnosti | 14 kal. dní |
| 4 | Bezplatné overenie opráv | Do 60 dní |

**Obmedzenie rozsahu a platnosti.** Správa opisuje nálezy z auditu 1.–12. apríla 2026. Audit je bodové overenie — odzrkadľuje stav v čase vykonania. Neskoršie zmeny môžu priniesť nové zraniteľnosti. Metodológia nie je vyčerpávajúca. Neidentifikované zraniteľnosti môžu existovať. Správa nie je certifikácia bezpečnosti. Odporúčame pravidelné opakovanie.