

PENETRATIONSTEST-BERICHT — AUSZUG (REDACTED)

Bericht-Nr.: SP-2025-4417 | Auftraggeber: VermieterCheck Solutions GmbH | Datum: 17. November 2025
Tester: [REDACTED] | Methode: Black-Box | Scope: ProspectScore Pro API (api.vermietercheck.de)

EXECUTIVE SUMMARY

Im Rahmen des beauftragten Black-Box-Penetrationstests der REST-API-Infrastruktur von ProspectScore Pro (VermieterCheck Solutions GmbH) wurde am 17. November 2025 eine kritische SQL-Injection-Schwachstelle (CVE-2026-0188) im Scoring-Backend identifiziert. Die Schwachstelle ermöglicht einem nicht authentifizierten Angreifer die vollständige Exfiltration der Mietinteressenten-Datenbank.

1. Kritischer Befund: CVE-2026-0188

CVSS v3.1 Score	9.8 (KRITISCH)
CVE-Nummer	CVE-2026-0188
Schwachstellen-Typ	SQL Injection (CWE-89)
Betroffene Komponente	REST-API /api/v3/prospect/search (ProspectScore Pro v3.0.4)
Angriffsvektoren	Network / Remotely Exploitable
Authentifizierung	Nicht erforderlich (unauthenticated)
Auswirkung Vertraulichkeit	Vollständig kompromittiert
Auswirkung Integrität	Vollständig kompromittiert
Auswirkung Verfügbarkeit	Hoch
DSGVO-Relevanz	Art. 32 DSGVO (Sicherheit der Verarbeitung), Art. 33 DSGVO (Meldepflicht)

2. Technische Beschreibung (Auszug — redacted)

Der API-Endpoint /api/v3/prospect/search akzeptiert einen URL-Parameter **q** (Suchanfrage), der ohne Eingabebereinigung direkt in eine PostgreSQL-14.2-Datenbankabfrage eingefügt wird. Die fehlende Parametrisierung (Prepared Statements) ermöglicht eine Blind-Time-Based-SQL-Injection.

HTTP-Request (anonymisiert / Beispiel-Payload):

```
GET /api/v3/prospect/search?q=1%27%20OR%20%27%27%3D%27%27 Host:
api.vermietercheck.de User-Agent: [REDACTED] [REDACTED — vollständige
Payload-Sequenz geschwächt] HTTP/1.1 200 OK {...response with full database
dump...}
```

3. Nachweis der Exfiltration

Die forensische Analyse der AWS-Server-Logs (CloudTrail, GuardDuty) ergab Anzeichen einer aktiven Ausnutzung der Schwachstelle in der Zeit vom 22.11. bis 24.11.2025 durch eine externe

IP-Adresse (Herkunft: [REDACTED — laufende Strafverfolgung]). Geschätzte exfiltrierte Datensätze:

Datenkategorie	Datensätze (ca.)	DSGVO-Sensitivität
Name + Adresse + E-Mail	142.300	Hoch
Schufa-Score + Negativmerkmale	98.400	Sehr hoch
Beruf + Einkommensdaten	139.100	Hoch
ProspectScore (KI-Ausgabe)	142.300	Sehr hoch
Familienstatus + Haushalt	88.700	Hoch
GESAMT	142.300 Personen	KRITISCH

4. Empfehlungen

Prio.	Massnahme	Frist
KRITISCH	Sofortige Implementierung Prepared Statements in allen DB-Abfragen	Sofort
KRITISCH	Deployment Web Application Firewall (AWS WAF) vor ProspectScore-API	Sofort
HOCH	Upgrade TLS 1.2 auf TLS 1.3	72h
HOCH	Vollständige Trennung Staging / Produktionsumgebung	7 Tage
HOCH	MFA fuer alle Admin-Accounts aktivieren	48h
MITTEL	Implementierung SAST/DAST in CI/CD-Pipeline	30 Tage

Quellen: DSGVO Art. 32, 33 — <https://dejure.org/gesetze/DSGVO> | CVE-2026-0188 — <https://cve.mitre.org> | OWASP SQL Injection — https://owasp.org/www-community/attacks/SQL_Injection | BSI IT-Grundschutz — <https://www.bsi.bund.de>