UITTREKSEL · FICTIEVE KLANT

SECTRICITY
OUTSMART HACKERS

UITTREKSEL UIT EEN PENTESTRAPPORT

Externe pentest webplatform en API

Acme Logistics NV · klantenportaal, publieke API en inlogflow

KLANT
Acme Logistics NV

TESTPERIODE
2 tot 13 maart

METHODE
OWASP WSTG · grey box

CLASSIFICATIE
Vertrouwelijk

01 · MANAGEMENTSAMENVATTING

Waar staat Acme vandaag?

Een aanvaller kan via de publieke API klantgegevens van andere klanten inzien. Twee bevindingen vragen een oplossing deze week; de rest kan in de normale planning.

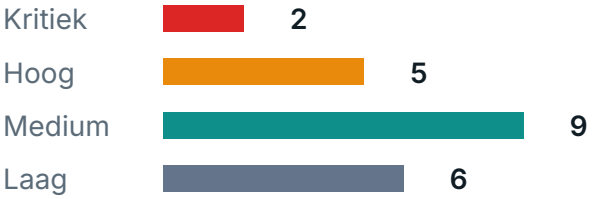
TOTAAL RISICO



Hoog

na hertest verwacht: laag

Bevindingen per ernst



22 bevindingen · alle handmatig bevestigd

Top 3 om eerst aan te pakken

KRITIEK	**Toegang tot orders van andere klanten**	API controleert eigenaar van order niet
KRITIEK	**Wachtwoordreset zonder limiet**	Resetcodes zijn te raden
HOOG	**Verouderde component in portaal**	Bekende kwetsbaarheid, update beschikbaar

Advies. Los de twee kritieke punten op en plan daarna de hertest. Die zit inbegrepen en bevestigt dat de oplossing werkt.

Deze week
2 kritieke punten oplossen

Binnen 30 dagen
5 hoge punten

Binnen 90 dagen
Medium en laag, daarna hertest

02 · BEVINDING SEC-01

Toegang tot orders van andere klanten

9.1
CVSS · KRITIEK

Onderdeel	Impact	Status
Publieke API	**Datalek klantgegevens**	**Open**

Wat we vonden

Door het ordernummer in de aanvraag te wijzigen, krijgt een ingelogde klant de orders, adressen en facturen van andere klanten te zien.

Bewijs

```
GET /api/v2/orders/10482 HTTP/1.1
Authorization: Bearer [redacted]

200 OK {"order":10482,"klant":"[redacted]","adres":"[redacted]"}
```

Zo los je het op

1. Controleer bij elke aanvraag of de order bij de ingelogde klant hoort.
2. Gebruik niet-voorspelbare order-ID's.
3. Log en alarmeer bij veel opeenvolgende ID's.

Waarom dit belangrijk is

Persoonsgegevens van alle klanten liggen open voor elke klant met een account. Dat is een datalek dat je onder de GDPR moet melden.

Hertest: **inbegrepen** binnen 90 dagen na het rapport

03 · OPLOSSINGSPLAN

Wat doe je wanneer?

Elke bevinding krijgt een termijn, op basis van ernst en hoe makkelijk een aanvaller ze kan misbruiken.

DEZE WEEK

Kritiek

- SEC-01 · Toegang tot orders van andere klanten
- SEC-02 · Wachtwoordreset zonder limiet

BINNEN 30 DAGEN

Hoog

- SEC-03 · Verouderde component
- SEC-04 · Sessie blijft geldig na uitloggen
- SEC-05 · Te ruime CORS-instelling

BINNEN 90 DAGEN

Medium en laag

- 9 medium bevindingen
- 6 lage bevindingen
- Hardening van headers

Wat al goed zit

- ✓ Sterke versleuteling van het verkeer
- ✓ Beheerpaneel niet bereikbaar vanaf internet
- ✓ Geen gevoelige gegevens in foutmeldingen

Hertest

Inbegrepen binnen 90 dagen na het rapport. We testen elke opgeloste bevinding opnieuw en bevestigen schriftelijk dat de fix werkt.