



# Dezvăluirea responsabilă a vulnerabilității





## Dezvăluirea responsabilă a vulnerabilității

Eleving Group se angajează să asigure securitatea informațională și protecția resurselor noastre de informații împotriva amenințărilor cibernetice. Încurajăm dezvăluirea responsabilă a securității vulnerabilităților, așa cum este stabilit în această politică, și salutăm orice deficiente raportate în securitatea serviciilor și resurselor noastre.

## Unde se aplică

Această politică se aplică următoarelor domenii:

- [\\*auto.mogo.md](https://auto.mogo.md)

Se exclude:

- autodiscover.auto.mogo.md
- eleving.com/.env, eleving.com/.aws/config și eleving.com/.aws/credential (Am implementat utilizarea fișierelor capcană, nu există informații valide aici)

Primim rapoarte despre vulnerabilități cum ar fi Cross-Site Scripting (XSS), injecții SQL, greșeli de criptare, executarea de cod de la distanță, erori de autentificare etc.

## Nu sunt autorizate următoarele tipuri de teste:

- Teste de prevenire a atacurilor de tip DoS, DDoS,
- Compromiterea credențialelor prin forță brută,
- Inginerie socială,
- Teste de acces fizic,
- Orice alte teste de vulnerabilitate non-tehnice.

## Mențiuni juridice

Acceptăm rapoarte de vulnerabilitate pentru domeniul de aplicare enumerat mai sus și suntem de acord să nu luăm măsuri legale împotriva persoanelor care:

- Respectă această politică în timpul operațiunilor de securitate Comply with this policy during security research;
- Testează produselor și serviciilor fără a afecta sistemele și datele noastre;
- Se abțin de la dezvăluirea către public a detaliilor vulnerabilității descoperite înainte de expirarea unui interval de timp convenit de comun acord.

Ne rezervăm dreptul de a accepta sau de a respinge orice raport privind orice vulnerabilitate și de a acționa în consecință, în conformitate cu normele și procedurile noastre interne.

## Cum puteți raporta?

Dacă ați descoperit o vulnerabilitate în resursele noastre informatice, vă rugăm să ne contactați la adresa [security@eleving.com](mailto:security@eleving.com) și să includeți următoarele informații:

- O descriere detaliată a vulnerabilității;
- Informații detaliate despre exploatarea vulnerabilității;
- Dacă este cazul, un link, screenshot-uri sau orice alte informații care ne ajută să identificăm vulnerabilitatea pe care ați descoperit-o.

## Ce așteptări avem?

Vă rugăm să rețineți că, în timpul verificării vulnerabilității, este esențial să respectați aceste reguli:

- Nu utilizați vulnerabilitatea detectată pentru a accesa sau a încerca să accesați informații care nu vă aparțin (doar pentru a dovedi existența vulnerabilității);
- Nu utilizați vulnerabilitatea detectată pentru a elimina sau modifica informațiile;
- Ne informați în timp util cu privire la vulnerabilitate și ne lăsați să rezolvăm vulnerabilitatea raportată înainte de a o face publică.

## Ce oferim noi?

Nu oferim compensații financiare, dar atunci când vulnerabilitatea raportată va fi rezolvată, putem oferi asistență și informații pentru publicația cercetătorului și putem promova contribuția acestuia, dacă s-a ajuns la un acord reciproc în acest sens.