Dezvăluirea responsabilă a vulnerabilității

mogo

Eleving Group se angajează să asigure securitatea informațiilor și protecția resurselor de informații împotriva amenințărilor cibernetice. Încurajăm semnalarea în mod responsabil a deficiențelor de securitate, așa cum este prevăzut în această politică și invităm orice persoană care efectuează cercetări în domeniul securității să raporteze deficiențele din domeniul serviciilor și resurselor noastre.

1 Scopul

Această politică se aplică următoarelor domenii:

- *automogo.ro

Excluderi:

- autodiscover.automogo.ro
- automogo.ro/.env, automogo.ro/.aws/config și automogo.ro/.aws/credential (Am implementat utilizarea fișierelor capcană, nu există informații valide aici)

Numărul de cereri nu trebuie să depășească 3 cereri pe secundă (aproximativ 10.000 de cereri pe oră). Așteptăm raportarea deficiențelor, cum ar fi Cross-Site Scripting (XSS), vulnerabilități la nivelul codului SQL, erori de criptare, executarea de cod rău intenționat de la distanță(remote execution), erori de autentificare etc.

2 Nu sunt autorizate următoarele tipuri de teste:

- Teste privind rezistența rețelei (DoS, DDoS).
- Compromiterea forțată a credențialelor,
- Prin instrumentele sociale în scop de înșelăciune,
- Testarea accesului fizic,
- Orice alte teste de vulnerabilitate non-tehnice.

3 Dispoziții finale

Orice raport de vulnerabilitate este acceptat pentru domeniul de aplicare menționat mai sus și ne angajăm să nu inițiem acțiuni legale împotriva persoanelor care:

- Respectă această politică în timpul verificărilor de securitate;
- Se angajează în testarea produselor și serviciilor fără ca sistemele și datele noastre să fie afectate;
- Se abțin de la expunerea publică a detaliilor privind vulnerabilitatea descoperită înainte de expirarea unui termen stabilit de comun acord.

Ne rezervăm dreptul de a accepta sau de a respinge orice raport cu privire la existența unor vulnerabilități și de a acționa în consecință, în conformitate cu normele și procedurile noastre interne.

4 Cum poți raporta?

Dacă se presupune că ai descoperit o vulnerabilitate în resursele noastre informatice, te rugăm să ne contactezi la adresa security@eleving.com și să precizezi următoarele informații:

- Descrierea detaliată a vulnerabilității;
- Informații detaliate despre exploatarea vulnerabilității
- Dacă este cazul, un link, capturi de ecran sau orice alte informații care ne ajută să identificăm punctual vulnerabilitatea pe care ai găsit-o.

5 Ce așteptări avem de la tine?

Te rugăm să reții că, în timpul cercetării privind orice vulnerabilitate, este esențial să respecți aceste reguli:

- Nu folosi vulnerabilitatea detectată pentru a accesa sau a încerca să accesezi informații care nu-ți aparțin (doar pentru a dovedi existența vulnerabilității);
- Nu folosi vulnerabilitatea detectată pentru a elimina sau modifica informațiile;
- Comunică-ne în timp util vulnerabilitatea identificată și permite-ne să o corectăm înainte de a o face publică.

6 Ce așteptări ai de la noi?

Nu oferim compensații financiare, dar odată ce problema semnalată va fi rezolvată, putem oferi asistență și informații despre realizarea cercetărilor și promovarea contribuției cercetătorului, dacă există un acord reciproc în acest sens.