Responsible vulnerability **disclosure**

mogo

Responsible vulnerability disclosure

Eleving Group is committed to ensuring the information security and protection of our information resources against cyber threats. We encourage responsible security vulnerability disclosure as set in this policy and welcome any security researchers to report security flaws in our services and resources.

Scope

This policy applies to the following domains:

- *cars.mogo.co.ke

Exclusion:

- autodiscover.cars.mogo.co.ke
- cars.mogo.co.ke/.env, cars.mogo.co.ke/.aws/config and cars.mogo.co.ke/.aws/credential (We have implemented the use of decoy files, no valid information here)

The number of requests must not exceed 3 requests per second (approximately 10,000 requests per hour). We expect reports about vulnerabilities such as Cross-Site Scripting (XSS), SQL injections, encryption flaws, remote code execution, authentication flaws, etc.

The following test types are not authorized:

- Network denial of service (DoS, DDoS) tests.
- Brute force credential compromise,
- Social engineering,
- Physical access testing,
- Any other non-technical vulnerability testing.

Legal Disclosure

We accept vulnerability reports for the scope listed above and we agree not to pursue legal action in good faith against individuals who:

- Comply with this policy during security research;
- Engage in testing products and services without harming our systems and data;
- Refrain from disclosing any discovered vulnerability details to the public before a mutually agreed-upon timeframe expires.

We reserve the right to accept or reject any reports on any vulnerabilities and act upon it in accordance with our internal rules and procedures.

How can you report?

If you believe that you have discovered a vulnerability in our information resources, please contact us at security@eleving.com and include the following information:

- A detailed description of the vulnerability;
- Detailed information about the exploitation of the vulnerability;
- If applicable, a link, screenshots, or any other information that helps us to identify the vulnerability you have found.

What do we expect from you?

Please note that during the vulnerability research, it is crucial that you follow these rules:

- You do not use the detected vulnerability to access or attempt to access information that does not belong to you (only to prove the existence of the vulnerability);
- You do not use the detected vulnerability to remove or modify the information;
- You inform us about the vulnerability in a timely manner and let us fix the reported vulnerability before going public with it.

What to expect from us?

We do not offer financial compensation, but when the reported vulnerability will be resolved, we may provide assistance and information for the researcher's publication and promote their contribution, if there has been a mutual agreement on it.