



Ответственное раскрытие
информации о недостатках
систем безопасности





Eleving Group (далее – Компания) стремится обеспечить информационную безопасность и защиту наших информационных ресурсов от киберугроз. Мы поощряем ответственное раскрытие информации об ошибках в системе безопасности, как это предусмотрено данной политикой, и приветствуем любых исследователей безопасности, которые сообщают о недостатках в наших услугах и ресурсах.

1 Область применения

Эта политика применяется к следующим доменам:

- *.auto.mogo.by

Исключение:

- autodiscover.auto.mogo.by
- eleving.com/.env, eleving.com/.aws/config и eleving.com/.aws/credential (Мы реализовали использование файлов-приманок, здесь нет достоверной информации.)

Мы ожидаем сообщений о таких ошибках, как Cross-Site Scripting (XSS), SQL injections, недостатки шифрования, недостатки аутентификации и т.д.

Цель тестирования: выявление недостатков систем безопасности для предотвращения угрозы несанкционированного доступа к информации и ее раскрытия.

Компания не дает разрешения на осуществление каких-либо действий с информацией, доступ к которой потенциально может быть получен в результате выявления ошибок в системах защиты информации.

2 Следующие типы тестов не разрешены:

- Сетевые проверки на отказ в обслуживании (DoS, DDoS),
- Компрометация учетных данных методом brute-force,
- Социальная инженерия,
- Тестирование физического доступа,
- Любое другое нетехническое тестирование на ошибки.

3 Юридическое раскрытие информации

Мы принимаем сообщения об ошибках в перечисленных выше областях и согласны не возбуждать судебных исков против лиц, которые:

- Соблюдают эту политику во время исследования безопасности;
- Занимаются тестированием продуктов и услуг без ущерба для наших систем и данных;
- Воздерживаются от разглашения информации об обнаруженной ошибке до истечения взаимно согласованного срока.

Мы оставляем за собой право принимать или отклонять любые сообщения о любых ошибках и действовать в соответствии с нашими внутренними правилами и процедурами.

4 Как вы можете сообщить?



Если вы считаете, что обнаружили ошибку в наших информационных ресурсах, пожалуйста, свяжитесь с нами по адресу security@eleving.com и укажите следующую информацию:

- Подробное описание ошибки (на английском, белорусском или русском языке);
- Подробная информация о работе ошибки;
- Если применимо, ссылку, скриншоты или любую другую информацию, которая поможет нам определить найденную вами ошибку.

Сообщение об ошибке может быть сделано анонимно.

Если в сообщении Вы указываете свои идентификационные сведения, то отправляя данное сообщение на указанный адрес электронной почты, Вы даете согласие на обработку нами Ваших персональных данных в соответствии с Политикой конфиденциальности, размещенной на сайте того.by, в целях и объеме, указанных в п. 3.6. данной Политики конфиденциальности.

5 Чего мы ждем от вас?

Обратите внимание, что во время исследования ошибки крайне важно соблюдать эти правила:

- Вы не используете обнаруженную ошибку для доступа или попытки доступа к информации, которая вам не принадлежит (только для доказательства существования ошибки);
- Вы не используете обнаруженную ошибку для удаления, копирования или изменения информации;
- Вы своевременно информируете нас об ошибке и позволяете нам устранить её, прежде чем обнародовать.

6 Чего ожидать от нас?

Мы не предлагаем финансовую компенсацию, но когда заявленная ошибка будет устранена, мы можем предоставить помощь и информацию для публикации тестирования, если на это есть взаимная договоренность.