Ответственное раскрытие уязвимостей

autotev

Eleving Group стремится обеспечить информационную безопасность и защиту наших информационных ресурсов от киберугроз. Мы поощряем ответственное раскрытие информации об уязвимостях системы безопасности, как указано в этой политике, и приглашаем всех аналитиков в области информационной безопасности сообщать о пробелах в системе безопасности наших служб и ресурсов.

Сфера применения

Настоящая политика применима к следующим доменам:

- *.autotev.lv

Исключение:

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

Мы ждем отчеты по оценке уязвимости, такие как межсайтовый скриптинг (XSS), внедрение SQL-кода, недостатки шифрования, удаленное выполнение кода, недостатки аутентификации и т. д.

Следующие типы тестов недопустимы:

- Сетевые проверки типа «отказ в обслуживании» (DoS, DDoS).
- Лобовая атака компрометации учетных записей.
- Психологическая атака.
- Тестирование физического доступа.
- Любое другое нетехническое тестирование уязвимостей.

Раскрытие информации на основании закона

Мы принимаем отчеты об уязвимостях для перечисленных выше целей и, основываясь на принципах добросовестности и взаимного доверия, обязуемся не возбуждать судебные иски против лиц, которые:

- соблюдают настоящую политику во время оценки безопасности;
- участвуют в тестировании продуктов и сервисов, не нанося вреда нашим системам и данным;
- не раскрывают сведения об обнаруженных уязвимостях общественности до истечения взаимно согласованного срока.

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

Как вы можете сообщить о раскрытии

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

- подробное описание уязвимости;
- подробная информация об использовании уязвимости;
- если применимо, ссылку, снимки экрана или любую другую информацию, которая поможет нам идентифицировать обнаруженную вами уязвимость.

Что мы ожидаем от вас

Обратите внимание, что во время изучения уязвимостей крайне важно соблюдать следующие правила:

- вы не используете обнаруженную уязвимость для доступа или попыток доступа к информации, которая вам не принадлежит (только для доказательства существования уязвимости);
- вы не используете обнаруженную уязвимость для удаления или изменения информации;
- вы своевременно сообщаете нам об уязвимости и позволяете нам исправить обнаруженную уязвимость, прежде чем сообщить о ней общественности.

Что ожидать от нас

Мы не предлагаем финансовую компенсацию, но когда уязвимость, о которой вы сообщили, будет устранена, мы можем предоставить помощь и информацию для публикации аналитиком и продвигать его вклад на основании взаимной договоренности.