ПОЛИТИКА РАСКРЫТИЯ УЯЗВИМОСТИ

1. Общая информация

Мы стремимся к тому, чтобы расширение Posttrack (далее – «Приложение»), для браузера Google Chrome,всегда было защищенным и безопасным. Когда выявляются уязвимости, мы прикладываем максимум усилий для их устранения. В этом документе описывается наша политика в отношении получения отчетов о потенциальных уязвимостях безопасности нашего Приложения, а также стандартная практика по информированию клиентов о проверенных уязвимостях.

Если вы считаете, что обнаружили уязвимость безопасности в Приложении, мы настоятельно рекомендуем вам сообщить нам о нём как можно быстрее и не публиковать уязвимость публично до тех пор, пока она не будет исправлена. Мы ценим вашу помощь, и мы просматриваем все отчеты и делаем все возможное, чтобы своевременно решать подобные проблемы. Чтобы поощрять предоставление нам информации об уязвимости безопасности, мы не будем обращаться к вам с иском в суд, если мы определим, что раскрытие информации соответствует нижеуказанным рекомендациям.

2. Руководство по раскрытию информации

Уведомлять и предоставлять нам информацию об уязвимости с предоставлением срока для устранения уязвимости не менее 1 (одного месяца**)** до публичного раскрытия.

Предоставить соответствующий уровень детализации уязвимости, чтобы мы могли идентифицировать и воспроизвести проблему. Детализация уязвимости должна включать целевые URL-адреса, пары запроса-ответа, скриншоты и/или другую информацию.

Приложите разумные усилия, чтобы избежать сбоев в обслуживании (например, DoS), проблемы конфиденциальности (например, доступ к данным пользователя Posttrack) и уничтожение данных при проведении исследований уязвимости.

Не запрашивайте компенсацию для отчетов об уязвимостях безопасности Приложения.

Не запускайте автоматические средства сканирования и не отправляйте нам вывод, не подтверждая, что проблема присутствует. Инструменты безопасности часто выводят ложные срабатывания, которые должны быть подтверждены.

3. Категории уязвимостей, которые мы поощряем

Нам в первую очередь интересно узнать о следующих категориях уязвимости:

- Кросс-сайт скриптинг (XSS);

- CSRF;
- SQL Injection;
- Проблемы, связанные с аутентификацией;
- Вопросы, связанные с авторизацией;
- Атаки перенаправления;
- Удаленное выполнение кода;
- Уникальные проблемы, которые не попадают в явные категории.

4. Категории уязвимости, которые мы не рассматриваем

Следующие категории уязвимостей рассматриваются вне сферы нашей программы раскрытия уязвимостей:

- Уязвимости SSL, связанные с конфигурацией или версией;
- Отказ в обслуживании (DoS);
- Злоупотребление функцией проверки подлинности пользователя;
- Брут;
- Флаг HTTPOnly не установлен на нечувствительные файлы cookie;
- CSRF;
- Проблемы, которые присутствуют только в старых браузерах/плагинах;
- Включен метод HTTP TRACE;
- Отчеты об уязвимостях, связанные с версиями веб-серверов, служб или фреймворков;
- Clickjacking на страницах без аутентификации;
- Отчеты об уязвимостях, требующие большого количества взаимодействия с пользователем для выполнения маловероятных или необоснованных действий, которые были бы более подходящим для социальной инженерии или фишинговой атаки, а не для уязвимости приложений (например, отключения функций защиты браузера, отправки критически важной информации злоумышленника для завершения атаки, направляя пользователя через определенную процедуру и требуя, чтобы они сами вводили вредоносный код и т. д.).

5. Изменения в политике раскрытия уязвимости

Мы оставляем за собой право в одностороннем порядке изменить политику раскрытия уязвимости, разместив соответствующую информацию на сайте. Поэтому мы просим вас периодически проверять наличие изменений.

6. Дополнительная информация

Если у вас есть вопросы по этой политике или хотели бы узнать больше о политике раскрытия уязвимости, отправьте электронное письмо на наш адрес posttrack@sloenka.com и мы свяжемся с вами.