ПОЛІТИКА РОЗКРИТТЯ ВРАЗЛИВОСТІ

1. Загальна інформація

Ми прагнемо до того, щоб розширення Posttrack (далі - «Додаток»), для браузера Google Chrome, завжди було захищеним і безпечним. Коли виявляються вразливості, ми докладаємо максимум зусиль для їх усунення. У цьому документі описується наша політика щодо отримання звітів про потенційні вразливості безпеки нашого Додатка, а також стандартна практика з інформування клієнтів про перевірені вразливості.

Якщо ви вважаєте, що виявили вразливість безпеки в Додатку, ми наполегливо рекомендуємо вам повідомити нам про неї якомога швидше і не публікувати вразливість публічно доти, поки вона не буде виправлена. Ми цінуємо вашу допомогу, і ми переглядаємо всі звіти, і робимо все можливе, щоб своєчасно вирішувати подібні проблеми. Щоб заохочувати надання нам інформації про вразливість безпеки, ми не будемо звертатися до вас з позовом до суду, якщо ми визначимо, що розкриття інформації відповідає вказаним нижче рекомендаціям.

2. Керівництво щодо розкриття інформації

Повідомляти і надавати нам інформацію про вразливість з наданням терміну для усунення вразливості не менше 1 (одного місяця) до публічного розкриття.

Надати відповідний рівень деталізації вразливості, щоб ми могли ідентифікувати та відтворити проблему. Деталізація вразливості повинна включати цільові URL-адреси, пари запиту-відповіді, скріншоти і/або іншу інформацію.

Докладіть розумні зусилля, щоб уникнути збоїв в обслуговуванні (наприклад, DoS), проблеми конфіденційності (наприклад, доступ до даних користувача Posttrack) та знищення даних при проведенні досліджень вразливості.

Не заявляйте виплату компенсації за звіти про вразливість безпеки Додатку.

Не запускайте автоматичні засоби сканування та не надсилайте нам висновок без підтвердження, що проблема існує. Інструменти безпеки часто видають помилкові спрацьовування, які повинні бути підтверджені.

3. Категорії вразливостей, які ми заохочуємо

Нам, в першу чергу, цікаво дізнатися про наступні категорії уразливості:

- Крос-сайт скриптинг (XSS);
- CSRF;

• SQL Injection;
• Проблеми, пов'язані з автентифікацією;
• Питання, пов'язані з авторизацією;
• Атаки перенаправлення;
• Віддалене виконання коду;
• Унікальні проблеми, які не потрапляють до явних категорій.

4. Категорії вразливості, які ми не розглядаємо

Наступні категорії вразливостей розглядаються поза сферою нашої програми розкриття вразливостей:

• Вразливості SSL, пов'язані зі зміною або версією;
• Відмова в обслуговуванні (DoS);
• Зловживання функцією перевірки автентичності користувача;
• Брут;
• Прапор HTTPOnly не встановлено на нечутливі файли cookie;
• CSRF;
• Проблеми, які присутні тільки в старих браузера /плагінах;
• Включений метод HTTP TRACE;
• Звіти про вразливість, пов'язані з версіями веб-серверів, служб або фреймворків;
• Clickjacking на сторінках без автентифікації;
• Звіти про вразливість, що вимагають великої кількості взаємодії з користувачем для виконання малоймовірних або необґрунтованих дій, які були б більш прийнятними для соціальної інженерії або фішингової атаки, а не для вразливості додатків (наприклад, відключення функцій захисту браузера, відправки критично важливої інформації зловмисника для завершення атаки, направляючи користувача через певну процедуру і вимагаючи самостійно вводити шкідливий код і т. п.).

5. Зміни в політиці розкриття вразливості

Ми залишаємо за собою право в односторонньому порядку змінити політику розкриття вразливості, розмістивши відповідну інформацію на сайті. Тому ми просимо вас періодично перевіряти наявність змін.

6. Додаткова інформація

Якщо у вас є питання щодо цієї політики, або ви хотіли б дізнатися більше про політику розкриття вразливості, надішліть листа електронною поштою на нашу адресу posttrack@sloenka.com, і ми зв'яжемося з вами.