ВРАЗЛИВІСТЬ СИСТЕМИ WORDPRESS

Антонюк В.В., к.ф-м.н., доц. Черних Е.П.
Національний технічний університет «ХПІ», Харків

На сьогоднішній день WordPress – це найпопулярніша та зручна блог-платформа для публікації статей та управління ними, на якій базується величезна кількість різних сайтів. Від загального числа сайтів, які використовують CMS-движки, її частка становить 60,4%. Відповідно зі статистикою 67,3% сайтів базується на останній версії даного програмного забезпечення. На жаль, базові налаштування не забезпечують достатнього рівня захисту. За тринадцять років існування веб-движка в ньому було виявлено 242 уразливості різного роду (без урахування вразливостей, знайдених в сторонніх плагінах і темах).

Плагін Jetpack – один з найпопулярніших для WordPress. Він включає велику кількість модулів (від створення галерей і розсилки в соціальні мережі до захисту від перебору паролів і підрахунку відвідуваності). За даними директорії WordPress.org, Jetpack має майже 25 мільйонів завантажень, і активний на понад 1 мільйон WordPress сайтів.

Дослідники з фірми веб-безпеки Sucuri знайшли «міжсайтовий скриптинг» (XSS), через який уразливості піддаються всі випуски Jetpack, починаючи з версії 2.0. Проблема розташована в модулі Shortcode Embeds, який дозволяє користувачам вбудовувати зовнішні відео, зображення, документи, твіти та інші ресурси в свій контент. Він може бути з легкістю використаний для введення шкідливого JavaScript-кода в коментарі. Так як JavaScript-код повторюється, він буде виконуватися в браузерах користувачів кожен раз, коли вони переглядають цей шкідливий коментар. Наприклад, він може використовуватися, щоб вкрасти ідентифікаційні куки, включаючи сеанс адміністратора; перенаправити відвідувачів до експлойтів або ввести спам пошукової оптимізації (SEO).

Для усунення цієї вразливості команда безпеки проекту WordPress скористалась механізмом автоматичних оновлень в ядрі WordPress, і за допомогою нього оновила Jetpack до останньої версії (в рамках встановленої гілки) на всіх сайтах з подібною підтримкою. Так само вчинили ряд хостинг-провайдерів.