Microsoft закрила критичну діру в Copilot: які дані могли викрасти хакери

ДМИТРУК АНДРІЙ — 17 Червня 2026, 15:46 2 Mins Read — ТЕХНОЛОГІЇ

У корпоративній платформі Microsoft 365 Copilot виявили небезпечну вразливість, яка дозволяла зловмисникам отримувати конфіденційні дані користувачів. Для запуску атаки жертві було достатньо натиснути на спеціально підготовлене посилання.

Про це пише Ars Technica.

Проблема пов’язана з особливостями роботи великих мовних моделей. Алгоритми не завжди здатні відрізнити справжні команди користувача від прихованих інструкцій, які можуть міститися в листах, документах або вебсторінках, що аналізуються штучним інтелектом.

Для захисту від витоку даних Microsoft впровадила спеціальні обмеження, які не дозволяють Copilot самостійно надсилати електронні листи або заповнювати вебформи. Проте дослідники зуміли знайти спосіб обійти цей захист, використовуючи стандартні HTML-теги, в які приховувалися конфіденційні дані.

Під час завантаження такого елемента браузер автоматично надсилав запит на сервер зловмисників, передаючи інформацію через системні журнали. Саме на цьому принципі базувалася атака SearchLeak, яку розробили фахівці з кібербезпеки компанії Varonis.

Схема починалася з надсилання користувачу спеціально сформованого посилання. У параметрі пошукового запиту містилася прихована команда для Copilot. Після переходу за посиланням система могла автоматично виконати інструкцію, наприклад знайти листи користувача та витягнути їхні заголовки.

Додатково дослідники виявили особливість потокового відображення відповідей Copilot. Під час генерації відповіді необроблений HTML-код на короткий час потрапляв у структуру сторінки браузера. Цього було достатньо, щоб браузер встиг відправити запит на сервер хакерів до моменту спрацювання захисних механізмів.

Ще одним елементом схеми став пошуковик Bing. Оскільки Copilot довіряє сервісам Microsoft, система безперешкодно надсилала запити через Bing, після чого дані могли перенаправлятися на сторонні ресурси, які контролювали зловмисники.

За оцінками експертів, наслідки могли бути особливо серйозними для корпоративних клієнтів Microsoft 365. Потенційно під загрозою опинилися коди двофакторної автентифікації, одноразові паролі з електронної пошти, внутрішні документи зі сховищ SharePoint і OneDrive, записи робочих зустрічей, календарі та конфіденційні нотатки.

У Microsoft вже випустили оновлення безпеки та усунули виявлені вразливості. Водночас експерти наголошують, що проблема довіри штучного інтелекту до зовнішнього контенту залишається актуальною, тому в майбутньому можуть з’являтися нові способи обходу захисних механізмів.

Помітили помилку у матеріалі? Повідомте редакцію: corrections@expert.in.ua

Microsoft Copilot кібербезпека хакери

ОСТАННІ НОВИНИ

СЬОГОДНІ

16:20 Безугла підтримала реформу Федорова: на що пропонують зробити ставку в армії

16:12 Стилісти назвали 5 речей для спеки: у чому буде комфортно навіть у найгарячіші дні

16:03 Земля стрімко дорожчає: в яких областях гектар став недоступною розкішшю

15:56 Науковці пояснили, чому шоколад із холодильника здається смачнішим

15:46 Microsoft закрила критичну діру в Copilot: які дані могли викрасти хакери

15:35 Названо прикмети літнього сонцестояння: чого боялися наші предки 21 червня

15:27 Названо 5 місць у Карпатах, які вражають більше за Говерлу: куди поїхати цього літа

15:23 Пенсіонери масово судяться через індексацію: чому виплати виявилися меншими

15:14 У Києві назвали кількість першокласників: чи вистачить місць у школах

15:06 Відстрочку можуть скасувати: кого першими хочуть відправити до війська

LOAD MORE

КАТЕГОРІЇ НОВИН

Всі новини
Україна
Політика
Економіка
Світ
Стиль життя
Авто
Технології
Суспільство
Здоров’я

ІНФОРМАЦІЯ

Про проект
Автори
Редакційна політика і стандарти
Політика використання ШІ
Політика конфіденційності
Правила коментування
Контакти

ТОВ «НОВА МЕДІА ГРУПА» © 2014—2026

Реєстрація R40-06871 у Реєстрі суб'єктів у сфері медіа

Адреса: 01014, м. Київ, вул. Звіринецька, 63

editor@expert.in.ua
corrections@expert.in.ua
reklama@expert.in.ua