**Wykryto lukę w popularnej wtyczce do WordPressa**

**We wtyczce do oprogramowania WordPress znaleziono lukę. Wadliwy plugin, Accelarator Mobile Pages (AMP), przyspiesza renderowanie stron internetowych na urządzeniach mobilnych. Wprawdzie wtyczka została usunięta z oficjalnych repozytoriów WordPressa, to jednak wcześniej pobrano ją już przeszło 100 tys. razy.**

21 października administratorzy stron www opartych na najpopularniejszym obecnie systemie zarządzanie treścią (content management system – CMS), którzy chcieli zainstalować wtyczkę za pośrednictwem panelu administracyjnego WordPressa, zobaczyli komunikat „Dnia 21 października wtyczka została wycofana i nie można jej pobrać”.

Powodem wycofania wtyczki było odkrycie błędu, który umożliwiał hakerom instalowanie na stronach opartych na WordPressie backdoorów, złośliwego kodu oraz zakładanie kont użytkownika na prawach administratora.

Na blogu autorów wtyczki pojawił się komunikat informujący, że została ona wycofana z oficjalnych repozytoriów tymczasowo i w przeciągu kilku dni, po usunięciu błędów w zabezpieczeniach, ponownie się pojawi. Autorzy nie ujawnili szczegółów dotyczących luki, poinformowali tylko, że może ona zostać wykorzystana do włamania na stronę przez osoby nie posiadające uprawnień administratora. Aktualnie dostępna już jest poprawiona, wolna od błędu wersja wtyczki, oznaczona numerem 0.9.97.20.

Zaskakująca jest opublikowana przez autorów wtyczki informacja, być może mająca na celu uspokojenie użytkowników, że do czasu wydania poprawki można z niej nadal korzystać. Rada zdecydowanie nie wzbudzała zaufania.

Badacze z WebARX, firmy zajmującej się zabezpieczeniem stron internetowych przed atakami, opublikowali więcej szczegółów nt. luki. Są one dostępne pod adresem: https://www.webarxsecurity.com/amp-plugin-vulnerability/

Autorzy Wordfence – popularnego firewalla i skanera antywirusowego dedykowanego dla WordPressa – potwierdzili, że luka była aktywnie wykorzystywana przez przestępców do ataku cross-site scripting, polegającym na wstrzyknięciu w treść strony złośliwego kodu skryptowego wykonywanego przez przeglądarkę internetową. W efekcie przestępcy mogli w atakowanym WordPressie tworzyć własnych użytkowników z prawami administratora, którym przydzielano najczęściej nazwę "supportuuser" (mogła zostać oczywiście zmieniona na inną).

WordPress jest obecnie najpopularniejszym CMS-em. Dostępne są dla niego tysiące wtyczek, które niestety mogą zawierać luki. Z obu tych powodów stał się dla hakerów jednym z najatrakcyjniejszych celów. Dlatego należy pamiętać o stałej konieczności aktualizowania zarówno samego WordPresa, jak i wykorzystywanych wtyczek. Zaleca się włączenie automatycznych aktualizacji wszędzie, gdzie jest to tylko możliwe.

„Samodzielny hosting stron na WordPressie wiąże się z wieloma korzyściami. Jednak pozostawienie opartej na tym popularnym systemie CMS witryny www bez opieki jest równoznaczne z udostępnieniem jej hakerom, którzy posiadają narzędzia do automatycznego wyszukiwania niezaktualizowanych stron ze znanymi lukami bezpieczeństwa. W efekcie narażasz na wymierne straty wizerunkowe i finansowe zarówno siebie, jak i Twoich klientów, którzy po odwiedzeniu zarażonej strony mogą stać się ofiarami przestępców” komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.