Bitdefender

# Cyberprzestępcy atakują miliony witryn internetowych opartych na WordPressie poprzez znane luki w zabezpieczeniach

07.06.2024

Zgodnie z najnowszymi doniesieniami badaczy bezpieczeństwa hakerzy wykorzystują obecnie luki w trzech bardzo popularnych wtyczkach WordPress, w tym WP Meta SEO, WP Statistics i LiteSpeed Cache. Eksperci do spraw cyberbezpieczeństwa apelują do właścicieli stron, aby sprawdzili, czy zainstalowali najnowsze aktualizacje.

## Cyberprzestępcy wykorzystują luki wtyczek w WordPressie

Jako jedna z najpopularniejszych platform treści internetowych na świecie, WordPress jest zawsze na celowniku cyberprzestępców. Jak każde oprogramowanie, wtyczki mogą mieć luki w zabezpieczeniach i w większości przypadków błędów, a już szczególnie tych krytycznych,

programiści szybko naprawiają problemy związane z bezpieczeństwem.

Niestety udostępnienie poprawki usuwającej lukę w zabezpieczeniach nie jest równoznaczne z jej wdrożeniem. Właściciele witryn czasami opóźniają instalację najnowszych poprawek. Właśnie na to liczą cyberprzestępcy, szukając swoich ofiar.

**Korzystasz z WordPress? Sprawdź, czy nie jesteś narażony na cyberatak**

Badacze bezpieczeństwa z Fastly odkryli, że celem skoncentrowanego ataku są obecnie trzy luki w zabezpieczeniach popularnych wtyczek: CVE-2024-2194, CVE-2023-6961 i CVE-2023-40000. Pomimo tego, że wszystkie te luki są stosunkowo nowe, to są już łatki naprawiające te problemy,

„Te luki występują w różnych wtyczkach WordPress i są podatne na ataki nieuwierzytelnionych przechowywanych skryptów między witrynami (XSS) z powodu nieodpowiedniego oczyszczenia danych wejściowych i ucieczki danych wyjściowych, co umożliwia atakującym wstrzykiwanie złośliwych skryptów” – wyjaśnili badacze. „Obserwowane przez nas ataki, których celem są te luki, wstrzykują znacznik skryptu wskazujący na zaciemniony plik JavaScript hostowany w domenie zewnętrznej”.

Rola skryptu jest prosta: pomóc atakującym w utworzeniu nowych kont administratorów, wprowadzić backdoory do stron internetowych i pomóc przestępcom w monitorowaniu zainfekowanych stron internetowych.

Dotyczy to wtyczki WP Statistics (wersja 14.5 i starsze), wtyczki WP Meta SEO (wersja 4.5.12 i starsze) oraz wtyczki LiteSpeed Cache (wersja 5.7.0.1 i starsze). Witryny korzystające z tych wtyczek są liczone w milionach, a duża ich część zawiera starsze wersje podatne na ataki.

„Administratorom stron internetowych zalecamy jak najszybsze uaktualnienie wszystkich wtyczek do najnowszych wersji i usunięcie wszelkich folderów, które mogły utworzyć starsze wersje wtyczek. Warto także przeprowadzić audyt bezpieczeństwa, a także sprawdzenie wszystkich plików w poszukiwaniu wstrzykniętego kodu. Ponadto przypominamy także o tym, aby zabezpieczyć urządzenie, które wykorzystujemy do obsługi WordPressa za pomocą skutecznego systemu antywirusowego” – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/cyberprzestepcy-atakuja-miliony-witryn-internetowych-opartych-na-wordpressie-poprzez-znane-luki-w-zabezpieczeniach/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 07.06.2024
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu

cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.