Bitdefender

Krytyczna luka w popularnej wtyczce WordPress to zagrożenie dla ponad 200 000 witryn

18.10.2023

Niedawno zauważono, że popularna wtyczka WordPress „Royal Elementor Addons and Templates” autorstwa WP Royal zawiera krytyczną lukę, która może narazić na ryzyko ponad 200 000 stron internetowych. Tego alarmującego odkrycia dokonały dwa zespoły ds. bezpieczeństwa WordPressa, WordFence i WPScan (Automattic), które zgłosiły, że hakerzy aktywnie wykorzystują tę lukę, powodując złowrogie bezpośrednie zagrożenie.

Wada wtyczki Wordpress – luka zero day

Luka oznaczona jako CVE-2023-5360 została sklasyfikowana w CVSS v3.1 z wynikiem 9,8, co oznacza, że jest „krytyczna”. Umożliwia nieuwierzytelnionym atakującym przesyłanie dowolnych plików na podatne strony internetowe dzięki luce w mechanizmie sprawdzania

rozszerzeń, zaprojektowanym w celu ograniczenia przesyłania tylko do niektórych dozwolonych typów plików.

Lukę wykorzystano jeszcze zanim dostawca zdążył wypuścić łatkę.

„Wtyczka Royal Elementor Addons and Templates dla WordPressa jest podatna na dowolne przesyłanie plików we wszystkich wersjach aż do 1.3.78 włącznie" – wynika z poradnika bezpieczeństwa WordFence. „Jest to spowodowane niewystarczającą walidacją typu pliku w handle_file_upload()funkcji wywoływanej przez AJAX, która umożliwia atakującym dostarczenie preferowanego rozszerzenia typu pliku do parametru allowed_file_typesze znakiem specjalnym, co pozwala przesłanemu plikowi ominąć listy filtrów. To sprawia, że nieuwierzytelnieni atakujący mogą przesłać dowolne pliki na serwer zagrożonej witryny, co może umożliwić zdalne wykonanie kodu."

Aktywna eksploatacja sięga końca sierpnia

Zespoły bezpieczeństwa prześledziły aktywne wykorzystanie luki od 30 sierpnia; jednakże począwszy od 3 października liczba ataków znacznie wzrosła.

Według doniesień WordFence zablokował w ciągu ostatniego miesiąca ponad 46 000 ataków wymierzonych w tę wtyczkę, natomiast WPScan zidentyfikował 889 przypadków wykorzystania tej luki przez atakujących. Sprawcy wdrażali różne szkodliwe ładunki, głównie skrypty PHP działające jako backdoory lub próbujące utworzyć fałszywe konta administratora.

Pilne wezwanie do aktualizacji do najnowszej wersji wtyczki

„Zespół Bitdefender zdecydowanie zaleca wszystkim użytkownikom wtyczki, której dotyczy problem, aktualizację do najnowszej wersji, aby zmniejszyć ryzyko ataku. Jednakże w przypadku tych, których witryny internetowe zostały już naruszone, sama aktualizacja wtyczki może nie zneutralizować infekcji. W takim wypadku konieczne może okazać się dokładne oczyszczenie wszystkich zasobów danej strony internetowej. Warto także zapewnić bezpieczeństwo komputerom, które są wykorzystywane przez administratorów danej witryny i zainstalować na nich skuteczny system antywirusowy, aby zminimalizować ryzyko zainfekowania ich za pomocą złośliwego oprogramowania” – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/krytyczna-luka-w-popularnej-wtyczce-wordpress-to-zagrozenie-dla-ponad-200-000-witryn/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 18.10.2023
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.