Bitdefender

Krytyczna luka w zabezpieczeniach wtyczki WordPress naraża 1 milion witryn

09.04.2024

Badacz cyberbezpieczeństwa AmrAwad odkrył niedawno krytyczną lukę w LayerSlider, wysokiej jakości wtyczce WordPress, z której korzysta ponad 1 milion stron internetowych. Luka naraża zainfekowane witryny internetowe na nieuwierzytelnione ataki polegające na wstrzykiwaniu kodu SQL, umożliwiając potencjalnym atakującym kradzież istotnych danych.

LayerSlider, podatna na ataki wtyczka, to popularne narzędzie, które pozwala właścicielom witryn tworzyć galerie obrazów, animacje i responsywne suwaki.

Krytyczna luka w zabezpieczeniach wtyczki Wordpress zgłoszona do programu Bug Bounty

Śledzona jako CVE-2024-2879, luka w zabezpieczeniach polegająca na wstrzykiwaniu SQL, która uzyskała wynik CVSS na poziomie 9,8 i jest oznaczona jako krytyczna, dotyczy wersji wtyczek od 7.9.11 do 7.10.0. Błąd ten został odkryty przez badacza AmrAwada 25 marca 2024 roku i przesłany do programu nagród za błędy firmy Wordfence zajmującej się bezpieczeństwem WordPress.

Jak czytamy w opisie wady, słabym punktem jest działanie wtyczki ls_get_popup_markup „z powodu niewystarczającej ucieczki od parametru dostarczonego przez użytkownika i braku wystarczającego przygotowania istniejącego zapytania SQL".

Luka zezwala na nieuwierzytelnione ataki typu SQL Injection

Ta luka we wtyczce Wordpress może pozwolić atakującym na dołączenie dodatkowych zapytań SQL do istniejących, co umożliwi im kradzież danych, w tym poufnych informacji o użytkowniku i skrótów haseł.

Co gorsza, ugrupowania cyberbprzestępcze mogą przeprowadzać te ataki bez uwierzytelniania na podatnych witrynach internetowych.

Po ataku polegającym na wstrzykiwaniu kodu SQL wyodrębnione dane mogą umożliwić atakującym złamanie poufnych informacji i przejęcie pełnej kontroli nad zaatakowaną witryną internetową.

Niebezpieczne strony internetowe mogą zostać uzbrojone

Całkowite przejęcie zainfekowanych witryn internetowych może poważnie wpłynąć na odwiedzających, którzy prawdopodobnie nie będą świadomi przejęcia kontroli przez złośliwy podmiot.

Według raportu Wordfence funkcja „prepare() sparametryzowałaby zapytanie SQL i uciekłaby z niego w celu bezpiecznego wykonania w WordPressie, zapewniając w ten sposób ochronę przed atakami polegającymi na wstrzykiwaniu kodu SQL".

Bitdefender zaleca natychmiastową aktualizację wtyczki

Po niezwłocznym powiadomieniu o problemie twórca wtyczki, Kreatura Team, w niecałe 48 godzin opublikował aktualizację zabezpieczeń.

Mankament został załatany w wersji 7.10.1 wtyczki LayerSlider; użytkownikom zaleca się aktualizację do najnowszej wersji, aby uniknąć ataków polegających na wstrzykiwaniu SQL, których celem są podatne na ataki wersje wtyczki.

„W przypadku ujawnienia luki we wtyczce Wordpress kluczowe jest jak najszybsze zainstalowanie łatki. Jeśli tego nie zrobimy, cyberprzestępcy mogą wykorzystać tę sytuację, rozsyłając niczego niepodejrzewającym odwiedzającym treści zawierające złośliwe oprogramowanie, potajemnie zbierając ich dane, prowadząc ich do formularzy phishingowych lub przekierowując do innych złośliwych miejsc docelowych" – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/krytyczna-luka-w-zabezpieczeniach-wtyczki-wordpress-naraza-1-milion-witryn/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 09.04.2024
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.