Bitdefender

Masowy cyberatak na krytyczną lukę w zabezpieczeniach wtyczki WordPress

19.07.2023

Według firmy Wordfence zajmującej się bezpieczeństwem WordPress krytyczne luki w popularnej wtyczce WordPress, WooCommerce Payments, zostały wykorzystane w poważnym cyberataku. Luka oznaczona jako CVE-2023-28121, która była celem masowej kampanii hakerskiej w ubiegłym tygodniu, ma krytyczną ocenę CVSS 9,8 na 10 i może umożliwić niezweryfikowanym atakującym przejmowanie kontroli nad witrynami internetowymi poprzez podszywanie się pod uprzywilejowanych użytkowników, takich jak administrator witryny.

Masowy cyberatak na krytyczną lukę w Wordpress

Atak osiągnął szczyt 16 lipca 2023 r., kiedy to przeprowadzono około 1,3 miliona ataków na 157 000 witryn. Ataki były skierowane głównie na wersje wtyczki WooCommerce Payments, począwszy od wersji 4.8.0 i

nowszych.

Złośliwi napastnicy wykorzystali tę lukę, dodając nagłówek X-WCPAY-PLATFORM-CHECKOUT-USER żądania i ustawiając go jako identyfikator konta użytkownika, pod którego chcieli się podszyć. Następnie WooCommerce przetwarzał żądanie tak, jakby pochodziło z rzeczywistego konta, zapewniając podmiotom odpowiedzialnym za zagrożenie odpowiednie uprawnienia.

Kolejnym krokiem hakerów było tworzenie nowych kont administratorów, lub instalacja innej wtyczki, bądź konsoli WP, która z uprawnieniami administratora uruchamiała złośliwy kod, wdrażała programy do przesyłania plików, a także tworzyła backdoory na zainfekowanych stronach internetowych.

Niepokojące jest to, że używanie narzędzia do przesyłania plików jako backdoora może utrzymywać się na zainfekowanych stronach internetowych nawet po usunięciu luki w zabezpieczeniach. Napastnicy identyfikowali przede wszystkim podatne witryny, próbując uzyskać dostęp do /wp-content/plugins/woocommerce-payments/readme.txt pliku. Jeśli się im to udawało, to rozpoczynali atak.

WooCommerce łata luki

WooCommerce odpowiedział na to zagrożenie, wydając 23 marca wersję 5.6.2 wtyczki, która usuwała lukę. Jednak pomimo zapewnień, że w tamtym czasie nie było żadnych znanych nadużyć, badacze bezpieczeństwa ostrzegali, że krytyczny charakter luki może

doprowadzić do ujawnienia się przypadków wykorzystania w przyszłości. Niestety, ta prognoza okazała się słuszna.

„W świetle ostatnich ataków na witryny Wordpressa zdecydowanie zaleca się administratorom witryn aktualizowanie ich witryn i wtyczek. W przypadkach, gdy aktualizacje wtyczek nie były instalowane przez dłuższy czas, zaleca się sprawdzenie i usunięcie wszelkich podejrzanych kont i plików PHP" – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/masowy-cyberatak-na-krytyczna-luke-w-zabezpieczeniach-wtyczki-wordpress/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 19.07.2023
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.