Bitdefender

Hakerzy wykorzystują porzuconą wtyczkę WordPress Eval PHP do włamań na strony internetowe

24.04.2023

Firma Sucuri zajmująca się cyberbezpieczeństwem odkryła nową falę ataków wymierzonych w witryny WordPress, która wykorzystuje porzuconą wtyczkę o nazwie Eval PHP.

Wtyczka nie była aktualizowana od ponad dekady, dzięki czemu stała się przydatnym narzędziem dla hakerów, którzy używają jej do umieszczania backdoorów na stronach internetowych w celu uzyskania nieautoryzowanego dostępu.

Czym jest Eval PHP?

Eval PHP został początkowo zaprojektowany, aby umożliwić

użytkownikom wykonywanie kodu PHP w postach i na stronach WordPress. Jednak wtyczka od dawna jest uważana za oprogramowanie porzucone, pozbawione aktualizacji i wsparcia swojego twórcy. Pomimo to nadal korzysta z niej wiele witryn WordPress, zwiększając swoją podatność na ataki.

Odkrycie przez Sucuri luki w Eval PHP ponownie zwróciło uwagę na niebezpieczeństwo związane z porzuconymi wtyczkami. Mogą one stanowić poważne cyberzagrożenie, ponieważ nie są aktualizowane, co pozwala hakerom wykorzystywać niezałatane luki w zabezpieczeniach i infekować strony internetowe.

Hakerzy wykorzystują porzuconą wtyczkę WordPress – jak się bronić?

W przypadku Eval PHP hakerzy wykorzystują wtyczkę do wstrzykiwania backdoorów do docelowych witryn WordPress. Udane infekcje pozwalają sprawcom uzyskać dostęp, wykraść poufne informacje lub całkowicie przejąć strony internetowe. Przestępcy często wykorzystują zainfekowane strony internetowe jako broń w ramach większych ataków, takich jak przeprowadzanie rozproszonych ataków typu „odmowa usługi” (DDoS) lub kampanie z wykorzystaniem złośliwego oprogramowania. Dlatego zespół Bitdefender zaleca, aby zawsze korzystać ze skutecznego oprogramowania antywirusowego, ponieważ atak może nastąpić ze strony, której się nie spodziewamy.

Co gorsza, mechanizmy exploita pozwalają hakerom utrzymać kontrolę

nad zainfekowanymi stronami internetowymi – nawet po usunięciu wtyczki.

„Chociaż omawiany „zastrzyk” wprowadza konwencjonalny backdoor do struktury plików, połączenie legalnej wtyczki i droppera backdoora w poście WordPress pozwala im łatwo ponownie zainfekować witrynę i pozostać w ukryciu” - czytamy w poradniku bezpieczeństwa Sucuri .

„Zespół Bitdefender zaleca użytkownikom WordPress natychmiastowe usunięcie nieaktualizowanej wtyczki Eval PHP ze swoich stron internetowych. Aby zmniejszyć ryzyko naruszenia bezpieczeństwa, warto zastąpić porzucone wtyczki tymi, które są wciąż czynnie wspierane. Ponadto właścicielom witryn zalecamy wdrożenie silnych środków bezpieczeństwa, takich jak stosowanie unikalnych, złożonych haseł, umożliwienie uwierzytelniania dwuskładnikowego, korzystanie ze skutecznych systemów antywirusowych i regularne monitorowanie podejrzanych działań” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/hakerzy-wykorzystuja-porzucona-wtyczke-wordpress-eval-php/

Data udostępnienia: 24.04.2023

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.