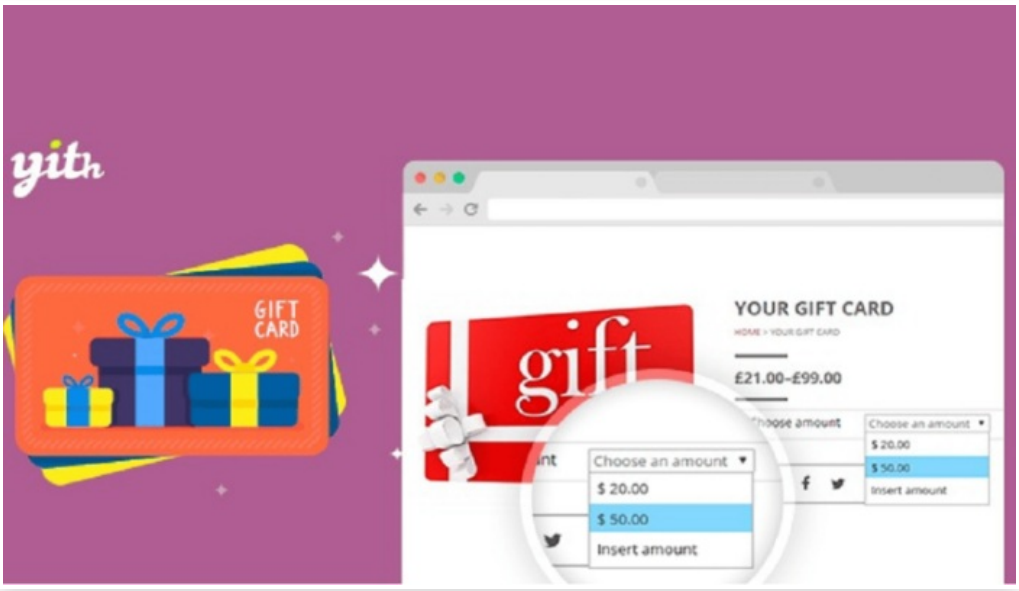
قراصنة يستغلون ثغرة خطرة في مكون إضافي شائع في ووردبرس



الاثنين 26 ديسمبر 2022 07:31 م

أفاد تقرير جديد بأن القراصنة يستهدفون بنشاط ثغرةً خطرةً في YITH WooCommerce Gift Cards Premium، وهو مكون إضافي لمنصة إدارة المحتوى ووردبرس WordPress يُستخدم في أكثر من 50,000 موقع ويب.

ومن خلال المكون YITH WooCommerce Gift Cards Premium، يبيع مشغلو مواقع الويب بطاقات الهدايا في متاجرهم عبر الإنترنت.

ويتيح استغلال الثغرة الأمنية، التي يجري تتبعها تحت المُعرِّف CVE-2022-45359، للقراصنة تحميل الملفات إلى المواقع الضعيفة والمعرضة للخطر، ومن ذلك: النصوص البرمجية الضارة التي تمكّن جهات التهديد الفاعلة من اختراق خوادم الويب، وشن هجمات إضافية.

وكان قد كُشف عن ثغرة CVE-2022-45359 للجمهور في 22 تشرين الثاني/ نوفمبر 2022، وقيل إنها تؤثر في جميع إصدارات المكون الإضافي حتى 3.19.0. وكان التحديث الأمني الذي عالج المشكلة هو الإصدار 3.20.0، ثم أطلق بائع الإضافة الإصدار 3.21.0، وهو الإصدار الذي يُوصى بتثبيته.

ولكن لا تزال العديد من المواقع تستخدم الإصدارات الأقدم وغير الحصينة، وقد ابتكر القراصنة بالفعل آليةً لمهاجمتها.

ووفقًا لخبراء أمان ووردبرس في Wordfence، فإن جهود الاستغلال جارية على نحو جيد، حيث يستفيد القراصنة من الثغرة الأمنية لتحميل الأبواب الخلفية على المواقع، وتنفيذ التعليمات البرمجية عن بُعد، بالإضافة إلى تنفيذ هجمات الاستيلاء.

واستغل القراصنة الثغرة باستخدام الهندسة العكسية لـ Wordfence في الهجمات، إذ اكتشفوا أن المشكلة تكمن في إحدى الوظائف الخاصة بالمكون الإضافي. وبسبب قصور هذه الوظيفة، فإنها تسمح للمهاجمين بإرسال طلبات نشر Post إلى الروابط الخاصة بالمشرفين، وذلك بهدف تحميل ملف PHP ضار قابل للتنفيذ على الموقع.

وأفاد المحللون أن معظم الهجمات وقعت في شهر تشرين الثاني/ نوفمبر قبل أن يتمكن المسؤولون من تصحيح الثغرة، ولكن لوحظت ذروة ثانية في 14 كانون الأول/ ديسمبر 2022.

ولا تزال محاولات الاستغلال جارية، لذا يوصى مستخدمو المكون الإضافي YITH WooCommerce Gift Cards Premium بالترقية إلى الإصدار 3.21 في أقرب وقت ممكن.