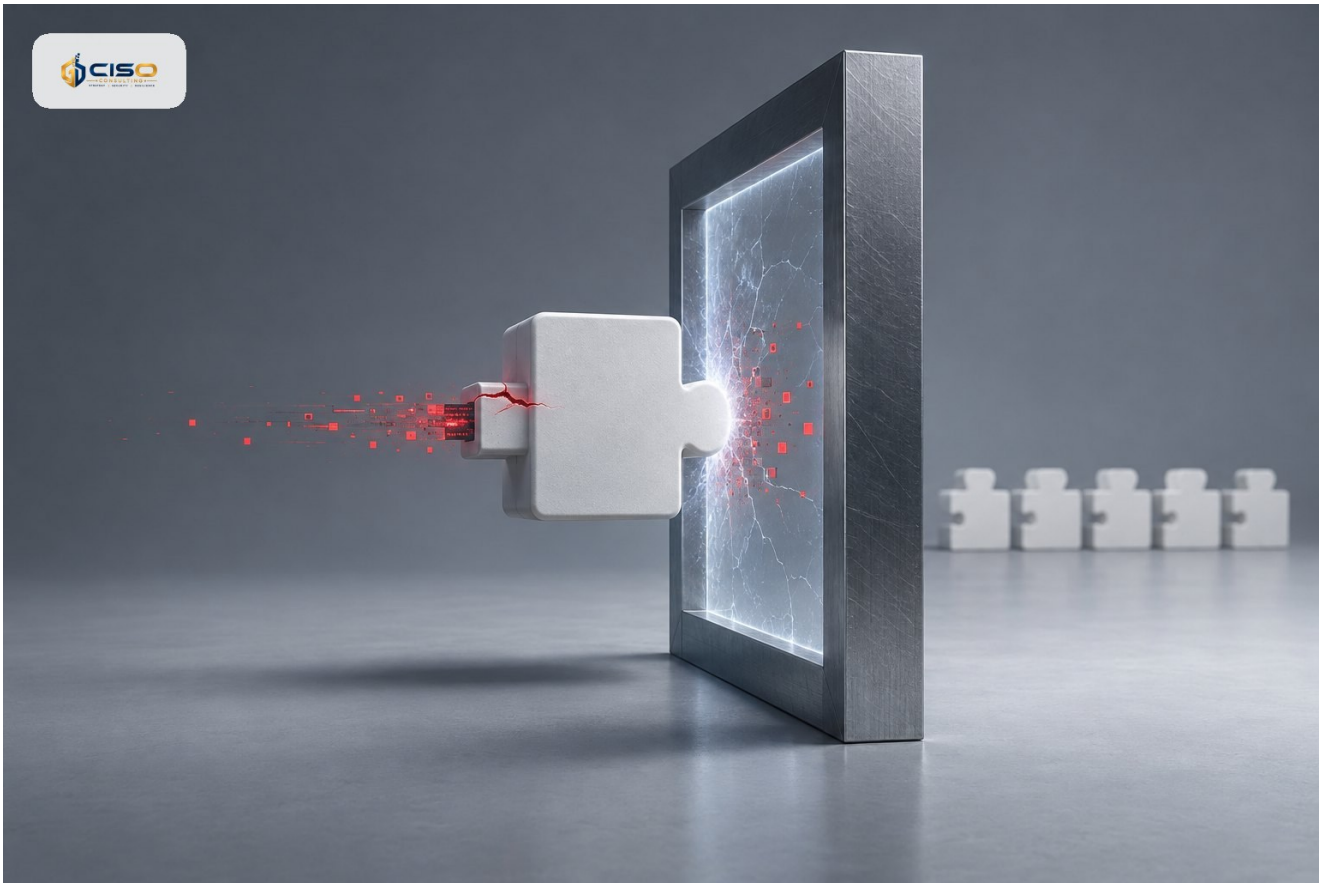
ووردبريس تحجب ست إضافات من WP Connect مزوّدة بباب خلفي قبل إصدارها



أزالت ووردبريس ست إضافات من WP Connect أُدخل عليها باب خلفي في 22 نوفمبر 2026 يتيح تنفيذ تعليمات برمجية عشوائية، إثر اشتباه باختراق حساب المطوّر، وحجبت الإصدارات الخبيثة قبل نشرها.

- أُزيلت ست إضافات من تطوير WP Connect من ووردبريس.
- أُدخل عليها باب خلفي في 22 نوفمبر 2026 يتيح تنفيذ تعليمات برمجية عشوائية.
- يُشتبه أن السبب اختراق حساب المطوّر.
- رصد فريق الإضافات في ووردبريس التهديد بشكل مستقل وحجبه قبل الإصدار الرسمي.
- صفحات الإضافات لم تعد متاحة.

ما حدث

أزالت ووردبريس ست إضافات من تطوير WP Connect. وبحسب التقرير، أُدخل على هذه الإضافات باب خلفي في 22 نوفمبر 2026 من شأنه إتاحة تنفيذ تعليمات برمجية عشوائية على أي موقع يستخدمها. ويُشتبه أن السبب هو اختراق حساب المطوّر.

ورصد فريق الإضافات في ووردبريس النشاط بشكل مستقل، وحجب الإصدارات الخبيثة قبل إصدارها رسمياً. ولم تعد صفحات الإضافات متاحة.

أهمية الخبر

يمثل ذلك مخاطر سلسلة التوريد، إذ يُستغل حساب ناشر موثوق لدفع شيفرة ضارة عبر قناة التحديث المعتادة. وقد يؤدي تنفيذ تعليمات برمجية عشوائية على خادم ويب إلى السيطرة على الموقع وتسرب البيانات وموطئ قدم داخل الشبكة.

لا يذكر المصدر أسماء الإضافات الست، ولا ما إذا تأثرت مواقع فعلًا، ولا كيفية اختراق الحساب. لذا ينبغي للمنشآت التحقق من تعرضها بدلًا من افتراض عدمه.

النهج الموصى به

الأولوية هي التأكد من وجود أي إضافة من WP Connect على مواقع ووردبريس التابعة للمنشأة أو شركاتها أو التي تديرها أطراف خارجية، والتعامل مع أي حالة كحادثة محتملة حتى يثبت العكس. وعلى المدى الأبعد، ينبغي إدراج أمن الإضافات وحسابات الناشرين ضمن إدارة الأطراف الثالثة وإدارة التغيير.

ما يجب فعله الآن

1. حصر جميع مواقع ووردبريس، بما فيها التي تديرها وكالات خارجية، وقائمة الإضافات المثبتة عليها.
2. التحقق من وجود أي إضافة من WP Connect وإزالتها أو تعطيلها.
3. عند وجودها، فحص الموقع بحثاً عن شيفرة غير متوقعة أو مستخدمين إداريين جدداً أو مهام مجدولة أو اتصالات صادرة، واتباع إجراءات الاستجابة للحوادث.
4. تدوير بيانات الاعتماد والمفاتيح على أي موقع متأثر.
5. إدراج فحص الإضافات ومراجعة تحديثاتها ضمن إدارة الأطراف الثالثة وإدارة التغيير.