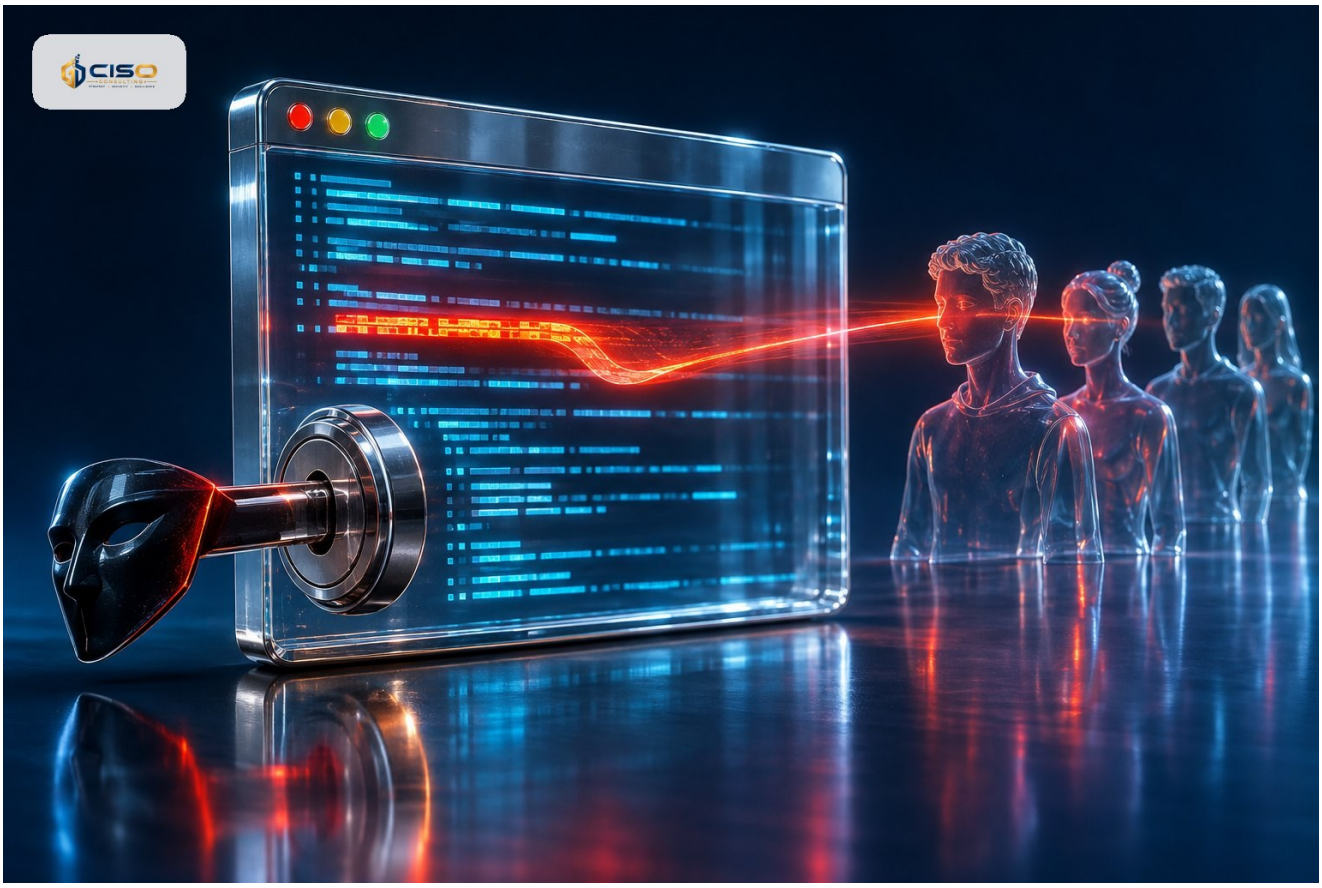
ثغرة في Optimizely Web Experimentation (CVE-2026-132224) قد تتيح للمهاجمين تعديل شيفرة JavaScript في المواقع



أدرجت CISA الثغرة CVE-2026-132224 في مسار إنشاء الحساب بمنتج Optimizely Web Experimentation، وتتيح انتحال مستخدمين وتعديل Project JavaScript لتُنفَّذ في متصفحات زوار المواقع.

- الثغرة من نوع التحكم الخارجي في بيانات الحالة الحرجة، وتقع في مسار إنشاء الحساب.
- يمكن للمهاجم انتحال مستخدمين حاليين لدى العميل وتعديل Project JavaScript.
- قد تُوزَّع شيفرة يتحكم بها المهاجم عبر أصول مستضافة لدى Optimizely وتُنفَّذ في متصفحات زوار المواقع المتأثرة.
- تطلب CISA تطبيق معالجات المورّد والالتزام بتوجيه BOD 26-04 ومتطلبات الفرز الجنائي، والموعد النهائي للجهات الفيدرالية 27-11-2026.

- إن لم تتوفر معالجات فتوجّه CISA بالتوقف عن استخدام المنتج.

أضافت CISA الثغرة CVE-2026-132224 إلى قائمتها. وتتعلق بمنتج Optimizely Web Experimentation، وتصنَّف ضمن التحكم الخارجي في بيانات الحالة الحرجة في مسار إنشاء الحساب.

ما الذي تتيحه الثغرة

وفق المصدر، يستطيع المهاجم انتحال مستخدمين حاليين لدى العميل ثم تعديل Project JavaScript. ولأن هذه الشيفرة تُوزَّع عبر أصول مستضافة لدى Optimizely، فقد ينتج عن الاستغلال الناجح تنفيذ شيفرة يتحكم بها المهاجم في متصفحات زوار المواقع المتأثرة.

وبالنسبة للجهات التي تستخدم المنتج في بواباتها العامة، لا يقتصر الأثر على حساب Optimizely نفسه، بل قد يصل إلى عملاء الموقع وزواره.

ما الذي تطلبه CISA

تطلب CISA تطبيق المعالجات وفق تعليمات المورّد، والالتزام بتوجيه BOD 26-04 الخاص بترتيب أولويات التحديثات الأمنية بحسب المخاطر، إضافة إلى متطلبات الفرز الجنائي. وفي الخدمات السحابية يُتَّبع التوجيه المعمول به ضمن BOD 26-04، أو يُتوقف عن استخدام المنتج إذا لم تتوفر معالجات. وعلى الجهات تقييم تعرّض كل أصل للإنترنت بنفسها. والموعد النهائي للجهات الفيدرالية هو 27-11-2026.

لا يذكر المصدر وجود استغلال فعلي ولا الإصدارات المتأثرة ولا إصلاحات محددة، لذا يُرجع إلى تعليمات المورّد لهذه التفاصيل.

نهج مقترح

يُنظر إلى الأمر بوصفه مخاطر سلسلة توريد للويب: تحقق من استخدام المنتج، وراجع من يملك صلاحية تعديل Project JavaScript، وافحص أي تغييرات غير متوقعة.

ما يجب فعله الآن

1. حصر جميع المواقع والبوابات التي تستخدم Optimizely Web Experimentation، بما فيها ما تديره فرق التسويق أو أطراف ثالثة.
2. تطبيق معالجات المورّد وتأكيد الحالة معه كتابيًا.
3. مراجعة Project JavaScript بحثًا عن تغييرات غير متوقعة أو غير مصرح بها، وفحص نشاط الحسابات والمستخدمين بحثًا عن مؤشرات انتحال.
4. تقييد وتدقيق من يملك صلاحية تعديل Project JavaScript، وفرض مصادقة قوية على تلك الحسابات.
5. عند غياب المعالجات، التخطيط لإيقاف استخدام المنتج وتوثيق قرار المخاطر.
6. حفظ السجلات ذات الصلة وإشراك فريق الاستجابة للحوادث عند اكتشاف تغييرات مشبوهة.