# اختطاف سكربتات Optimizely Web Experimentation المحمّلة في مواقع 178 جهة على الأقل



أعلنت Optimizely أن مهاجماً استغل ثغرة لزرع شيفرة خبيثة في سكربتات تُحمَّل في مواقع عملائها. وذكرت Report URI أن زوار 178 جهة على الأقل، منها CNN وBBC وZoom، تلقوها.

- استغل مهاجم ثغرة في Optimizely Web Experimentation بحسب إعلان Optimizely.
- زُرعت شيفرة خبيثة في بعض السكربتات التي تحمّلها مواقع العملاء من الخدمة.
- ذكرت Report URI، التي ترصد سكربتات المواقع، أن زوار 178 جهة على الأقل تلقوا الشيفرة.
- من المواقع المذكورة CNN وBBC وZoom.
- يشير العنوان إلى سكربت لسرقة بيانات البطاقات وحزم استغلال لنظام iOS، ولا يتضمن المقتطف المتاح تفاصيل عن سلوك الشيفرة.

أعلنت Optimizely أن مهاجماً استغل ثغرة في منتجها Web Experimentation وأدخل شيفرة خبيثة في بعض السكربتات التي تحمّلها مواقع العملاء من الخدمة. وكشفت الشركة الحادثة صباح اليوم.

وتفيد Report URI، وهي جهة ترصد السكربتات التي تشغّلها المواقع، بأن زوار مواقع 178 جهة على الأقل تلقوا الشيفرة أمس، ومن الجهات التي سمّتها CNN وBBC وZoom.

## ما هو معروف

يذكر عنوان المصدر أن السكربتات المصابة أوصلت سكربتاً لسرقة بيانات البطاقات وحزم استغلال لنظام iOS. إلا أن النص المتاح لنا جزئي، ولذلك لا تتوفر تفاصيل عن سلوك الشيفرة أو الثغرة المستغلة أو الإجراءات التي أصدرتها Optimizely للمعالجة. ويحسن انتظار إشعار المورّد نفسه قبل استخلاص نتائج.

## لماذا يهم ذلك

تبرز الحادثة مخاطر السكربتات الخارجية؛ فالشيفرة المقدَّمة من منصة المورّد تعمل بثقة الموقع الذي يضمّنها، وأي اختراق لدى المورّد يصل إلى زوار جميع العملاء دفعة واحدة. وعلى الجهات التي تعالج مدفوعات البطاقات أو تخدم مستخدمي الجوال أن تعدّ هذه السكربتات جزءاً من سطح الهجوم لديها.

## الخطوات المقترحة

على المؤسسات أن تتحقق أولًا هل تستخدم Optimizely Web Experimentation في أي موقع أو تطبيق عام، ثم تتبع إرشادات المورّد وتراجع ما حمّلته صفحاتها خلال الفترة المعلن عنها.

## ما يجب فعله الآن

1. تحقق مما إذا كان أي موقع أو بوابة أو تطبيق عام لديكم يستخدم Optimizely Web Experimentation.
2. اتبعوا إشعار Optimizely وطبّقوا أي معالجة تنشرها.
3. راجعوا سجلات خادم الويب ومدير الوسوم وسياسات المحتوى بحثاً عن تغييرات في السكربتات خلال الفترة المعلن عنها.
4. إذا تأثرت صفحات الدفع فأبلغوا الجهة المستحوذة وقيّموا تعرّض بيانات البطاقات وفق PCI DSS.
5. أبقوا جرداً محدثاً للسكربتات الخارجية وفكروا بضوابط سلامة مثل سياسة أمان محتوى مقيِّدة.