College Board تؤكد وقوع اختراق بعد تغييرات غير مصرح بها لكلمات المرور



أفادت College Board بأن مهاجمين استخدموا أدوات مدعومة بالذكاء الاصطناعي لاكتشاف ثغرة في صفحة تسجيل الحسابات المهنية، فوصلوا إلى أنظمة التسجيل وCSS Profile. ويجري التحقيق في اختراق مرتبط لدى مورّد خارجي.

- أبلغ طلاب عن إشعارات تغيير كلمة المرور دون طلب منهم يوم عيد الشكر، وظهرت جميعها من الموقع الجغرافي نفسه.
- تقول College Board إن المهاجمين استغلوا ثغرة في صفحة تسجيل الحسابات المهنية، اكتُشفت باستخدام أدوات مدعومة بالذكاء الاصطناعي.
- تمكّن المهاجمون من بدء إعادة تعيين كلمات المرور والاطلاع على بيانات تسجيل أساسية مثل الأسماء والبريد الإلكتروني.
- تعرّض مورّد خارجي يخزّن طلبات المساعدة المالية لاختراق منفصل يُعتقد أنه مرتبط بالحادثة، ولا

يزال نطاقه قيد التحقيق.

- أُوقف التسجيل الجديد والوصول إلى CSS Profile مؤقتاً، ولم يُعلن عدد الحسابات المتأثرة.

أكدت College Board، المنظمة غير الربحية المسؤولة عن اختباري SAT وAP وخدمة CSS Profile للمساعدات المالية، وقوع اختراق بعد أن أبلغ طلاب عن تغيير كلمات مرورهم دون طلب منهم.

ما الذي حدث

تفيد المنظمة بأن المهاجمين وصلوا إلى الأنظمة المستخدمة لإنشاء الحسابات الجديدة وتقديم طلبات CSS Profile. وذكرت لموقع BleepingComputer أنهم استخدموا أدوات مدعومة بالذكاء الاصطناعي لاكتشاف ثغرة في صفحة تسجيل الحسابات المهنية ثم استغلوها. وأتاح ذلك بدء إعادة تعيين كلمات المرور لبعض المستخدمين والاطلاع على بيانات تسجيل أساسية مثل الأسماء والبريد الإلكتروني.

وتقول College Board إن الأمر يمس نسبة صغيرة من المستخدمين، وإنها تعمل مع خبراء خارجيين لتحديد النطاق. ولم يُطَّلع، بحسب ما ذُكر، على مستودع نتائج الاختبارات وأسئلتها. كما تعرّض مورّد خارجي يخزّن طلبات المساعدة المالية لاختراق منفصل في الوقت نفسه يُعتقد أنه مرتبط بالحادثة، ولا تزال البيانات المتأثرة قيد التحديد.

الاستجابة والأثر

أُوقف مؤقتاً التسجيل الجديد والوصول إلى CSS Profile، بينما يستمر دخول المستخدمين الحاليين. وتعتزم المنظمة إصدار عمليات إعادة تعيين إضافية لكلمات المرور للطلاب المتأثرين والمراقبين وغيرهم من المهنيين، وقد تتبعها عمليات أخرى. ولم تعلن عدد الحسابات المتأثرة ولا موعد استعادة الخدمات، وتعمل على حلول تساعد الأسر على استكمال طلباتها قبل المواعيد النهائية.

أهمية الحادثة

تبيّن الحادثة أن ثغرة في صفحة تسجيل هامشية قد تقود إلى الاستيلاء على الحسابات، وأن مورّداً يحتفظ بمستندات حساسة قد يوسّع نطاق التعرض. وبما أن المهاجمين استخدموا أدوات ذكاء اصطناعي لاكتشاف الثغرة، فينبغي افتراض أن مثل هذه الثغرات قد تُكتشف أسرع من السابق.

ما يجب فعله الآن

1. مراجعة أمان مسارات التسجيل العامة وإعادة تعيين كلمات المرور، بما في ذلك تحديد معدلات الطلبات والتحقق والتنبيه عند عمليات إعادة التعيين الجماعية.
2. اختبار البوابات المواجهة للإنترنت بحثاً عن الثغرات المنطقية، ومنها الصفحات قليلة الاستخدام مثل تسجيل الحسابات المهنية أو حسابات الشركاء.
3. تحديد الأطراف الثالثة التي تخزّن بيانات عملائكم الحساسة، وطلب شروط الإبلاغ عن الحوادث وأدلة الأمان لديها.
4. إعداد خطة لإعادة تعيين بيانات الاعتماد على نطاق واسع تشمل إشعارات العملاء وتغطية الدعم خلال العطل ونهايات الأسبوع.

5. إن كانت جهتكم تعالج بيانات شخصية، فتحقق مما إذا كانت حادثة مماثلة ستستوجب الإشعار بموجب نظام حماية البيانات الشخصية (PDPL) والمتطلبات القطاعية مثل الإطار الاستشاري للأمن السيبراني للبنك المركزي السعودي (SAMA CSF).