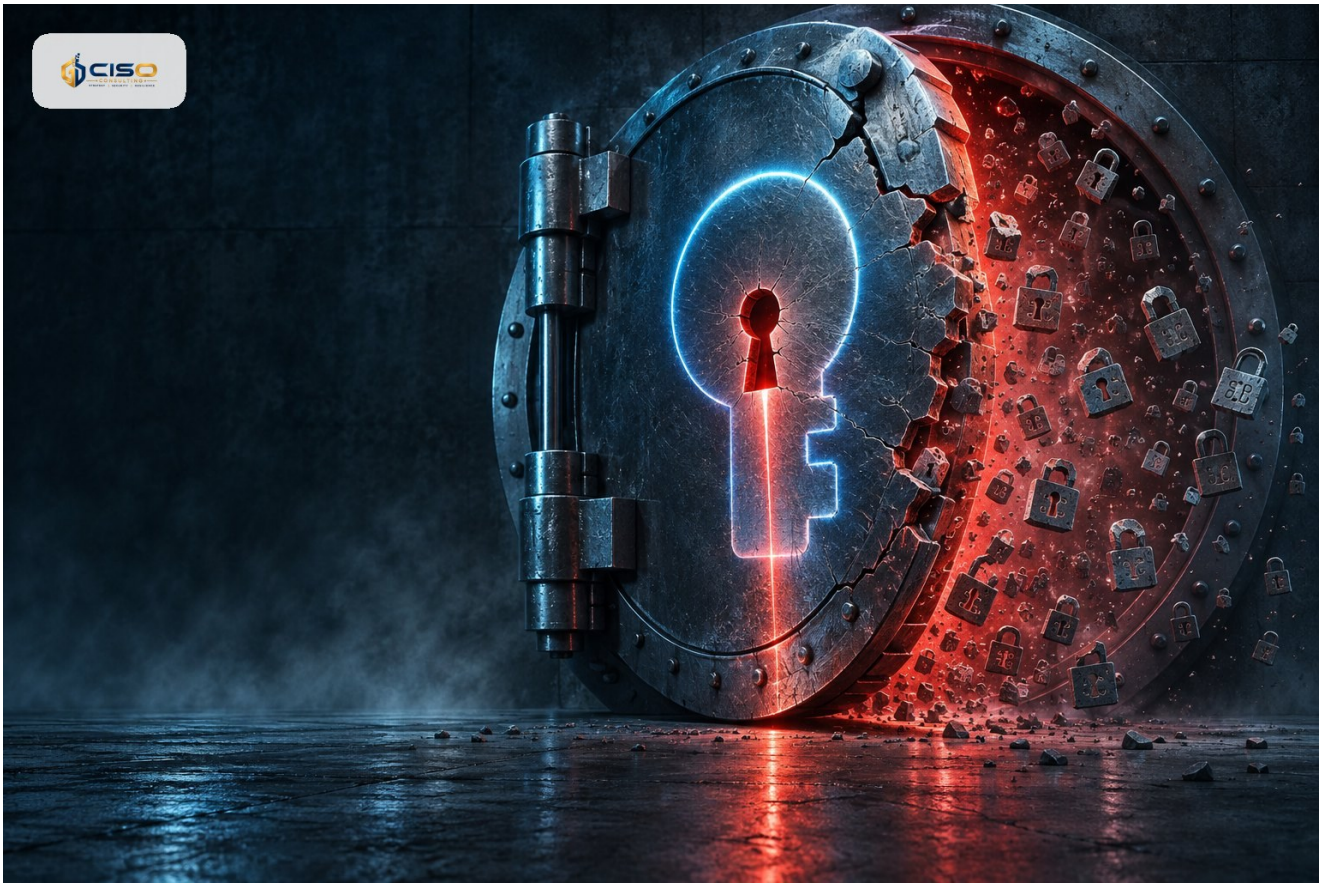
# اختراق مدير كلمات المرور mSecure: دعوة العملاء إلى إعادة ضبط بيانات الدخول



طلبت mSeven Software من عملاء mSecure الحاليين والسابقين تغيير كلمات المرور وإعادة ضبط المصادقة الثنائية وإزالة مفاتيح المرور، بعد هجوم سيبراني أفادت التقارير بأنه كشف قاعدة بيانات مشفرة للعملاء.

- تحذّر mSeven Software، الجهة المطوّرة لمدير كلمات المرور mSecure، عملاءها بعد هجوم سيبراني.
- أفادت التقارير بأن الهجوم كشف قاعدة بيانات مشفرة للعملاء.
- التوصية تشمل العملاء الحاليين والسابقين على حد سواء.
- الخطوات المطلوبة: تغيير كلمات المرور وإعادة ضبط المصادقة الثنائية وإزالة مفاتيح المرور.

## ما الذي أُعلن

حذّرت mSeven Software، الشركة المطوّرة لمدير كلمات المرور mSecure، عملاءها الحاليين والسابقين من ضرورة اتخاذ خطوات وقائية عقب هجوم سيبراني. وبحسب ما نُشر، فقد كشف الحادث قاعدة بيانات مشفرة للعملاء.

وتتمثل توصيات الشركة في تغيير كلمات المرور وإعادة ضبط المصادقة الثنائية وإزالة مفاتيح المرور. وتنطبق هذه التوصيات على العملاء السابقين كما تنطبق على الحاليين، لذلك قد يحتاج من توقف عن استخدام المنتج إلى اتخاذ الإجراءات نفسها.

## ما لم يرد في المصدر

لا يتضمن النص المتاح تفاصيل فنية إضافية، مثل نطاق البيانات المعنية أو التسلسل الزمني للحادث. ينبغي للجهات عدم افتراض ما لم يُذكر، ومتابعة إشعارات الشركة المطوّرة كلما جرى تحديثها.

## الأهمية للجهات المنظّمة

تحتفظ مديرات كلمات المرور ببيانات الدخول التي تحمي أنظمة أخرى. وحتى إن كانت البيانات المخزنة مشفرة، فإن إعادة الضبط الاحترازية تحدّ من الفترة التي قد تفيد فيها أي بيانات مكشوفة المهاجم. وقد يستخدم الموظفون كذلك حسابات شخصية أو قديمة لإدارة كلمات المرور في أعمالهم، وغالباً لا تراها فرق الأمن.

يُستحسن اعتماد استجابة هادئة ومنظمة: التحقق من استخدام المنتج داخل الجهة، وطلب إكمال خطوات إعادة الضبط التي أوصت بها الشركة، وإعطاء الأولوية للحسابات ذات الصلاحيات العالية أو الوصول عن بُعد.

## ما يجب فعله الآن

1. التحقق من استخدام الموظفين لـ mSecure، بما في ذلك الحسابات الشخصية المستخدمة في الدخول إلى أنظمة العمل.
2. طلب تغيير كلمات المرور وإعادة ضبط المصادقة الثنائية وإزالة مفاتيح المرور من مستخدمي mSecure الحاليين والسابقين وفق توصية الشركة.
3. إعطاء الأولوية لإعادة الضبط في الحسابات ذات الصلاحيات العالية وحسابات الوصول عن بُعد والحسابات الحرجة.
4. مراجعة سجلات الدخول بحثاً عن نشاط غير معتاد في الحسابات التي كانت بياناتها مخزنة في mSecure.
5. متابعة إشعارات mSeven Software وتحديث الإرشادات الداخلية عند صدور تفاصيل جديدة.