اختراق مزعوم لمنصة Cloud One التابعة لسلاح الجو الأمريكي ضمن موجة حوادث اتحادية



أفادت تقارير باختراق منصة Cloud One التابعة لسلاح الجو الأمريكي عبر ثغرة غير محددة، ضمن سلسلة حوادث طالت جهات اتحادية أمريكية. وحذّر مكتب FBI من أداة ARTEX للهجمات المؤتمتة بالذكاء الاصطناعي.

- تفيد رويترز بأن الاختراق اكتُشف خلال الشهر الماضي أثناء ترقية المنصة، مما عطّل ترحيل التطبيقات وتحديثات البرمجيات.
- بحسب مصدر، استغل المهاجمون ثغرة برمجية غير محددة؛ ولا تزال هوية المهاجمين ونطاق الهجوم وسرقة أي بيانات مجهولة.
- أُفيد أيضاً باختراق نظام NCIC لدى FBI ونظام تحليل مصادر مفتوحة لدى CIA وشبكة FinCEN، والعلاقة بينها غير واضحة.
- يقول FBI إن ARTEX، إطار اختبار اختراق مفتوح المصدر بالذكاء الاصطناعي، استُخدم منذ

أغسطس 2026 على الأقل، وبعض الاختراقات بلغت صلاحيات مرتفعة في أقل من ثلاث ساعات.

- لا يُعرف إن كان ARTEX قد استُخدم ضد سلاح الجو أو FBI أو FinCEN.

أفادت تقارير، نقلًا عن رويترز عبر BleepingComputer، باختراق Cloud One، منصة الحوسبة السحابية المؤسسية لسلاح الجو الأمريكي. أُطلقت المنصة عام 2017 وتتيح لجهات وزارة الدفاع استضافة تطبيقات العمليات وشؤون الأفراد والإمداد والصيانة.

ما هو معروف

اكتُشف الاختراق خلال الشهر الماضي أثناء ترقية المنصة، مما عطّل ترحيل التطبيقات وتحديثات البرمجيات. وقال مصدر إن المهاجمين استغلوا ثغرة برمجية غير محددة، وربما تعرضت معلومات عملياتية ولوجستية حساسة. وأُفيد باستدعاء القيادة السيبرانية الأمريكية. ولا يزال المهاجمون ونطاق الهجوم وسرقة البيانات مجهولة. وامتنع سلاح الجو عن التعليق على حالة الأنظمة.

يأتي ذلك بعد حوادث أخرى: مركز معلومات الجريمة الوطني لدى FBI، ونظام تحليل مصادر مفتوحة لدى CIA (وأثر أيضاً في ODNI وNGA)، وتحقيق FinCEN في دخول غير مصرح به. ولا يُعرف إن كانت مترابطة.

أدوات هجوم بالذكاء الاصطناعي

أُفيد بأن اختراق CIA تم باستخدام ARTEX، الذي يقول FBI إن جهات متعددة استخدمته منذ أغسطس 2026 على الأقل ضد أهداف حكومية ودفاعية وصحية ومالية وتقنية. يؤتمت الإطار اكتشاف الثغرات ورفع الصلاحيات وسرقة البيانات، ويرتبط بنماذج ذكاء اصطناعي خارجية. وبلغت بعض الاختراقات صلاحيات مرتفعة في أقل من ثلاث ساعات. ورصد باحثون أكثر من 1600 وحدة إدارة مكشوفة لـ ARTEX بحلول مطلع نوفمبر.

لا يذكر المصدر ما إذا استُخدم ARTEX ضد سلاح الجو أو FBI أو FinCEN. وينبغي للمؤسسات السعودية اعتبار ذلك دافعاً لمراجعة نوافذ التغيير في المنصات السحابية وسرعة التصحيح والكشف، لا تهديداً مؤكداً لبيئاتها.

ما يجب فعله الآن

1. مراجعة الضوابط الأمنية حول ترقيات المنصات السحابية وعمليات الترحيل المخطط لها، بما في ذلك المراقبة أثناء نوافذ التغيير.
2. التأكد من إعطاء أولوية لتصحيح البرمجيات المكشوفة للإنترنت والمستضافة سحابياً وقياس السرعة مقارنة بزمن المهاجمين.
3. اختبار قدرة الكشف والاستجابة على احتواء رفع الصلاحيات خلال ساعات لا أيام.
4. مراجعة الوصول ذي الصلاحيات المرتفعة إلى المنصات السحابية وفرض مصادقة قوية وتسجيلًا كافياً.
5. إطلاع مجلس الإدارة وفريق الاستجابة للحوادث على الهجمات المؤتمتة بالذكاء الاصطناعي وتأكيد مسارات التصعيد إلى الجهات الوطنية المختصة.