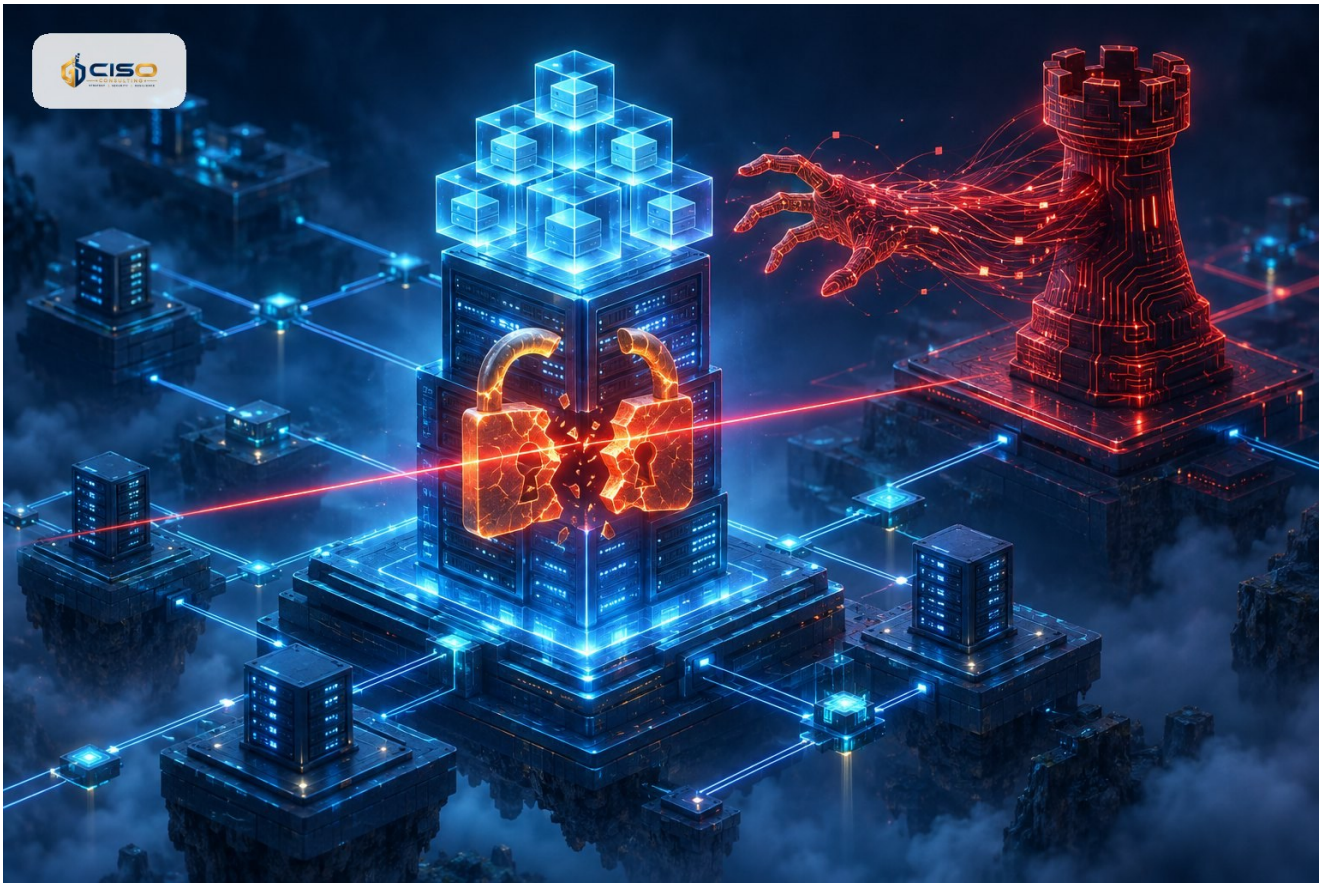
مجموعة مرتبطة بالصين تستغل ثغرة يوم الصفر الحرجة في VMware vCenter (CVE-2026-123890)



نُسب إلى مجموعة تجسس يُشتبه بارتباطها بالصين، تُعرف بـ Armory Castle، استغلال ثغرة تجاوز المصادقة الحرجة (CVSS 9.8) CVE-2026-123890 في VMware vCenter Server كيوم صفر في أوائل سبتمبر 2026.

- تتبع الجهة باسم Armory Castle، المعروفة سابقاً بـ UNC5221، ويُشتبه بارتباطها بالصين.
- الثغرة هي CVE-2026-123890 بتصنيف CVSS 9.8 في VMware vCenter Server.
- تتعلق بتجاوز المصادقة في VMware Directory Service.
- نُسب الاستغلال كيوم صفر إلى أوائل سبتمبر 2026.
- يشير عنوان التقرير إلى أن الهجمات أدت إلى صلاحيات إدارية وسرقة بيانات.

نُسب إلى مجموعة تجسس إلكتروني يُشتبه بارتباطها بالصين، تُعرف باسم Armory Castle وكانت تُتتبع سابقاً باسم UNC5221، استغلال ثغرة حرجة في VMware vCenter Server كيوم صفر، وذلك وفق التقرير في أوائل سبتمبر 2026.

ما المعروف حتى الآن

تحمل الثغرة الرمز **CVE-2026-123890** وتصنيف CVSS بدرجة 9.8، وهي ثغرة تجاوز مصادقة في VMware Directory Service. ويذكر عنوان التقرير أن الاستغلال منح المهاجمين صلاحيات إدارية وأتاح سرقة البيانات. والمقتطف المتاح لنا مبتور، لذلك لا تتوفر هنا تفاصيل مؤكدة عن الإصدارات المتأثرة أو توفر التصحيح أو الضحايا أو مؤشرات الاختراق.

أهمية الخبر

يدير vCenter Server البنية الافتراضية للمؤسسة. وتجاوز المصادقة في خدمة أساسية، مع استغلاله قبل توفر إصلاح، يعني إمكانية الوصول إلى طبقة الإدارة بصلاحيات عالية دون بيانات اعتماد صحيحة. وعلى الجهات التي تستخدم VMware التعامل مع الأمر كأولوية ومتابعة إرشادات الشركة المصنعة فور صدورها.

النهج المقترح

تأكدوا من استخدام vCenter في بيئتكم، وقيّدوا الوصول إليه، وراقبوا أي نشاط إداري غير معتاد. وراجعوا نشرة الشركة المصنعة لمعرفة التصحيح أو الحلول المؤقتة قبل إجراء أي تغيير، ووثّقوا القرارات لأغراض التدقيق.

ما يجب فعله الآن

1. حصر جميع نسخ vCenter Server وتسجيل إصداراتها.
2. تقييد الوصول الشبكي إلى واجهات إدارة vCenter بشبكات إدارية مخصصة.
3. متابعة نشرة الشركة المصنعة وتطبيق التصحيح أو الحل المؤقت عند تأكيده.
4. مراجعة سجلات vCenter وخدمة الدليل بحثاً عن دخول إداري غير متوقع أو تغييرات في الحسابات.
5. تدوير بيانات الاعتماد ذات الامتيازات عند رصد نشاط مشبوه، والتصعيد عبر مسار الاستجابة للحوادث.