مجموعة «Armory Castle» المرتبطة بالصين تستغل ثغرة يوم صفر في VMware vCenter



تفيد Dark Reading بأن مجموعة تهديد مرتبطة بالصين تُعرف باسم Armory Castle ربما كانت تملك ثغرة يوم صفر أخرى في VMware vCenter عند صدور آخر تحديثات أمنية كبرى للمنتج.

- يصف المصدر الجهة المهاجمة بأنها مجموعة تهديد مرتبطة بالصين تحمل اسم Armory Castle.
- الهدف هو VMware vCenter، طبقة الإدارة للبيئات الافتراضية.
- يرجَّح أن المجموعة كانت تملك ثغرة يوم صفر تالية أثناء موجة التحديثات الأمنية السابقة لـ vCenter.
- لا يتضمن المقتطف المتاح رقم CVE أو حالة التصحيح أو تفاصيل عن الضحايا.

ما الذي ورد في التقرير

تفيد Dark Reading بأن مجموعة تهديد مرتبطة بالصين، يُشار إليها باسم Armory Castle، تستهدف VMware vCenter عبر ثغرة يوم صفر. ووفق التقرير، يُرجَّح أن المجموعة كانت تملك ثغرة يوم صفر تالية أثناء صدور موجة التحديثات الأمنية الكبرى السابقة لـ vCenter.

المعلومات المتاحة لنا محدودة؛ فهي لا تذكر رقم CVE ولا ما إذا كان هناك تصحيح من الشركة المصنِّعة ولا الإصدارات المتأثرة ولا الجهات المستهدفة. لذلك نمتنع عن الجزم في هذه النقاط.

أهمية الخبر

يدير vCenter الأجهزة الافتراضية والمضيفات التي تعمل عليها غالباً الأنظمة الأساسية للمؤسسة. وقد يمنح اختراق هذه الطبقة المهاجم نطاق وصول واسعاً، ولذلك تستحق منصة الإدارة هذه الاهتمام حتى قبل اكتمال التفاصيل التقنية. كما أن الإشارة إلى امتلاك المجموعة ثغرة أخرى احتياطية تعني أن تطبيق آخر التحديثات وحده قد لا يكفي.

النهج المقترح

نوصي باعتبار الخبر دافعاً لمراجعة كيفية إتاحة vCenter ومراقبته، ومتابعة نشرات VMware للحصول على الإصلاحات والإجراءات التخفيفية المؤكدة. وتجنَّبوا التغييرات الطارئة المبنية على افتراضات، وتصرفوا وفق إرشادات الشركة عند صدورها.

ما يجب فعله الآن

1. حصر جميع نسخ vCenter والتحقق من إصداراتها ومستوى التصحيح فيها.
2. حصر واجهات إدارة vCenter في شبكات إدارية مخصصة ومنع إتاحتها عبر الإنترنت.
3. متابعة نشرات VMware الأمنية وتطبيق الإصلاحات أو الإجراءات التخفيفية فور تأكيدها.
4. رفع مستوى التسجيل والتنبيه على عمليات المصادقة والنشاط الإداري في vCenter.
5. التأكد من حداثة النسخ الاحتياطية للأجهزة الافتراضية الحرجة وعزلها واختبارها.