ثغرة يوم الصفر CVE-2026-123890 في VMware vCenter استغلتها مجموعة مرتبطة بالصين قبل صدور الإصلاح



أصدرت Broadcom إصلاح الثغرة الحرجة CVE-2026-123890 في vCenter (CVSS 9.8) التي استغلتها مجموعة مرتبطة بالصين لأكثر من شهرين. لا يوجد إصلاح علني للإصدار 7.0، لذا يلزم التحديث والتحقق من أي اختراق.

- الثغرة CVE-2026-123890 (CVSS 9.8) موجودة في VMware Directory Service وتتيح لمهاجم عن بُعد ودون مصادقة الحصول على جلسة موثّقة بصلاحيات مسؤول.
- تفيد Google بأن الاستغلال استمر أكثر من شهرين قبل صدور الإصلاح، وتربطه Mandiant بمجموعة Armory Castle (المعروفة أيضاً بـ Warp Panda وسابقاً UNC5221).
- بدأ الوصول الأولي عبر ثغرة يوم الصفر CVE-2026-102764 في BeyondTrust Remote Support، ثم الانتقال إلى أجهزة Linux ثم vCenter.

- الإصلاحات متاحة في vCenter بالإصدارات 9.1.1.0200 و9.0.2.0200 و8.0 U3m، أما الإصدار 7.0 فانتهى دعمه العام في أكتوبر 2025 ولا يوجد له إصلاح علني.
- نشرة Broadcom لا تشير إلى الاستغلال الفعلي، ولذلك لا يكفي التحديث وحده ويُنصح بفحص الأنظمة بحثاً عن اختراق.

أفادت Google بأن مجموعة تجسس يُشتبه في ارتباطها بالصين استغلت ثغرة يوم صفر في VMware vCenter لأكثر من شهرين قبل أن تصدر Broadcom الإصلاح يوم الخميس. تحمل الثغرة الرمز CVE-2026-123890 وتصنيف CVSS بقيمة 9.8، وتقع في VMware Directory Service، ويمكن لمهاجم عن بُعد بلا بيانات اعتماد استغلالها للحصول على جلسة موثّقة بصلاحيات مسؤول.

ما رصدته Mandiant

تنسب Mandiant، التي أبلغت Broadcom عن الثغرة، النشاط إلى مجموعة Armory Castle المعروفة أيضاً باسم Warp Panda والمتتبَّعة سابقاً باسم UNC5221. وبحسب النتائج، دخلت المجموعة أولًا عبر CVE-2026-102764، وهي ثغرة يوم صفر في BeyondTrust Remote Support صدر إصلاحها حديثاً، ثم انتقلت إلى أجهزة Linux في الشبكة الداخلية واستهدفت vCenter في أوائل سبتمبر.

استخدم المهاجمون أداة مخصصة تسمى Bonesaw لسرقة قاعدة بيانات LMDB واستخراج مواد توقيع SAML وإنشاء حساب مسؤول في الدخول الموحد (SSO). ثم استُخدمت أداة ثانية لتزوير رموز SAML وزُرعت أبواب خلفية. كما استولوا على مفتاح التشفير الرئيسي لـ vCenter وبيانات اعتماد قاعدة البيانات، ثم انتقلوا إلى مضيف ESXi. وقد شُغّلت Bonesaw ضد خادم vCenter سبق تحديثه لمعالجة CVE-2026-59309، وهي ثغرة منفصلة لتجاوز المصادقة أُعلن عنها في يوليو.

توفر الإصلاحات

أصدرت Broadcom إصلاحات في vCenter بالإصدارات 9.1.1.0200 و9.0.2.0200 و8.0 U3m. وتقول Mandiant إن Bonesaw تعمل ضد الإصدارين x.7 وx.8. أما الإصدار 7.0 فقد انتهى دعمه العام في أكتوبر 2025 ولا يتوفر له إصلاح علني. ولا تذكر نشرة Broadcom الاستغلال الفعلي للثغرة.

ويوصي Charles Carmakal، الرئيس التقني في Mandiant، بتطبيق التحديثات وفحص الأنظمة بحثاً عن مؤشرات اختراق في الوقت نفسه.

ما يجب فعله الآن

1. حصر جميع منصات vCenter وإصداراتها، والترقية إلى 9.1.1.0200 أو 9.0.2.0200 أو 8.0 U3m بحسب الحالة.
2. بالنسبة إلى vCenter 7.0 الذي لا يتوفر له إصلاح علني، التخطيط للانتقال إلى إصدار مدعوم وتقييد الوصول الشبكي إليه في الأثناء.
3. إجراء فحص استقصائي حتى على الخوادم المحدّثة: البحث عن حسابات مسؤول SSO غير متوقعة، ونشاط SAML مزوّر، وأبواب خلفية مجهولة، ووصول غير معتاد إلى ESXi.
4. عند الاشتباه باختراق، اعتبار مواد توقيع SAML ومفتاح التشفير الرئيسي لـ vCenter وبيانات اعتماد قاعدة البيانات مكشوفة والتخطيط لتدويرها.

5. التأكد من تحديث BeyondTrust Remote Support لمعالجة CVE-2026-102764، ومراجعة أجهزة الوصول عن بُعد وأجهزة Linux الداخلية.
6. إبلاغ الجهات المعنية بالحوادث المؤكدة عبر مسار التصعيد المعتمد، بما في ذلك الهيئة الوطنية للأمن السيبراني والجهة التنظيمية القطاعية عند الاقتضاء.