

ثغرة حرجية في Docker Hub سمحت بانتحال هوية المستخدمين والتلاعب بالصور



كشفت Docker عن ثغرة حرجية في Docker Hub سمحت للمهاجمين بانتحال هوية المستخدمين والتلاعب بصور الحاويات من خلال سوء معالجة رموز الوصول الشخصية أثناء تحويل الحسابات إلى مؤسسات.

- الثغرة CVE-2026-105445 سمحت للمهاجمين بإعادة تعيين رموز الوصول الشخصية دون موافقة المستخدم أثناء تحويل الحساب إلى مؤسسة
- تمكن المهاجمون من سحب أو دفع أو حذف صور الحاويات في مستودعات الأهداف، مما خلق مخاطر على سلسلة التوريد
- أصلحت Docker الثغرة خلال أربع ساعات من التأكيد ولم تجد دليلاً على الاستغلال عبر 304,000 عملية دفع تم تحليلها
- تم إلغاء تفعيل الرموز المنقولة في 8 أكتوبر 2026، والمنصة تطلب الآن موافقة المستخدم قبل

تفاصيل الثغرة

كشفت Docker عن الثغرة CVE-2026-105445، وهي ثغرة حرجية في Docker Hub مكّنت المهاجمين من انتحال هوية المستخدمين الشرعيين والتلاعب بصور الحاويات. نشأت الثغرة من المعالجة غير السليمة **لرموز الوصول الشخصية** أثناء تحويل الحسابات الفردية إلى مؤسسات.

تضمن أسلوب الهجوم إنشاء حساب برمز وصول شخصي، ثم تحويل ذلك الحساب إلى مؤسسة، وتعيين مستخدم مستهدف كمالك للمؤسسة. كانت منصة Docker Hub تعيد تعيين رمز المهاجم للمستخدم المستهدف دون تغيير الرمز السري أو الحصول على موافقة. عمل الرمز المعاد تعيينه بصلاحيات الهدف على مستوى السجل، مما سمح للمهاجمين بسحب أو دفع أو حذف الصور في المستودعات التي يمكن للضحية الوصول إليها.

تداعيات سلسلة التوريد

صنّفت Docker الثغرة على أنها حرجية بسبب تأثيرها المحتمل على سلاسل توريد البرمجيات. كان بإمكان المهاجمين نشر صور حاويات ضارة تحت أسماء مستخدمين شرعيين، مما يقوض الثقة في نظام الحاويات البيئي. لم تمنح الثغرة وصولاً إلى وحدة التحكم عبر الويب ولم تسمح بتغيير بيانات اعتماد الحساب أو كلمات المرور أو إعدادات المصادقة الثنائية، مما حدّ من نطاق الاختراق لعمليات السجل فقط.

المعالجة والتحقيق

تم إدخال الثغرة في 26 أغسطس 2024، وظلت موجودة حتى تلقت Docker تقريراً في 30 سبتمبر 2026. نشرت الشركة إصلاحاً في بيئة الإنتاج خلال أربع ساعات من التأكيد. فحصت Docker ما يقارب 304,000 عملية دفع تمت باستخدام رموز منقولة وحللت صوراً عامة عالية المخاطر، ولم تجد دليلاً على الاستغلال. تم إخطار المستخدمين المتأثرين في 2 أكتوبر، وتم إلغاء تفعيل الرموز المنقولة في 8 أكتوبر، باستثناء الحالات التي طلب فيها المالكون صراحة الاحتفاظ بها. تطلب المنصة الآن موافقة المستخدم قبل تسمية الأفراد كمالكين للمؤسسات ولم تعد تنقل الرموز أثناء التحويل.

ما يجب فعله الآن

- مراجعة جميع حسابات Docker Hub ورموز الوصول الشخصية المستخدمة داخل مؤسستك لتحديد أي تحويلات أو عمليات نقل رموز غير مصرح بها
- فحص صور الحاويات التي تم سحبها أو دفعها بين 26 أغسطس 2024 و8 أكتوبر 2026 للتحقق من سلامتها وأصالتها
- تطبيق عمليات التحقق من صور الحاويات بما في ذلك التحقق من التوقيع قبل النشر في بيئات الإنتاج
- وضع سياسات تتطلب سير عمل موافقة صريحة لتحويلات الحساب إلى مؤسسة على جميع منصات التطوير
- تحديث إجراءات الاستجابة للحوادث لتشمل سيناريوهات اختراق سلسلة التوريد التي تتضمن سجلات

الحاويات

6. النظر في تطبيق سجلات حاويات خاصة مع ضوابط وصول معززة للتطبيقات الحرجة ضمن أطر الهيئة الوطنية للأمن السيبراني أو مؤسسة النقد العربي السعودي