

Docker Hub تعالج ثغرة حرجية في المصادقة تتيح التلاعب بالصور عبر حسابات المستخدمين



أصلحت Docker ثغرة حرجية في Docker Hub سمحت للمهاجمين بنشر أو سحب أو حذف صور الحاويات باسم مستخدم آخر، دون وجود دليل على استغلالها.

- أصلحت Docker ثغرة حرجية في المصادقة بمنصة Docker Hub في 30 سبتمبر 2024
- سمحت الثغرة لمستخدم بنشر أو سحب أو حذف صور الحاويات باسم مستخدم آخر
- كانت الثغرة موجودة في ميزة تحويل الحسابات الشخصية إلى مؤسسات
- نشرت Docker تنبيهاً أمنياً في 12 أكتوبر 2024 يؤكد عدم وجود دليل على استغلال الثغرة
- استمرت الثغرة لمدة عامين تقريباً قبل معالجتها

تفاصيل الثغرة

عالجت Docker ثغرة حرجية في المصادقة بمنصة Docker Hub سمحت بوصول غير مصرح به عبر حسابات المستخدمين إلى صور الحاويات. الثغرة التي أُصلحت في 30 سبتمبر 2024 مكّنت المهاجم من نشر أو سحب أو حذف صور الحاويات تحت هوية مستخدم آخر. كشفت Docker عن المشكلة في تنبيه أمني نُشر في 12 أكتوبر 2024.

كانت الثغرة موجودة في ميزة تحويل الحسابات التي تحوّل حسابات Docker Hub الشخصية إلى حسابات مؤسسية. استمرت الثغرة لمدة عامين تقريباً قبل أن تحددتها Docker وتحلها. وفقاً لتنبيه المورد، لم يجد التحقيق الداخلي أي دليل على استغلال الثغرة فعلياً خلال هذه الفترة.

الآثار على المؤسسات الخاضعة للتنظيم

بالنسبة للمؤسسات في المملكة التي تستخدم **سجلات الحاويات** كجزء من سلسلة توريد البرمجيات، يؤكد هذا الحادث مخاطر المصادقة والتحكم في الوصول الكامنة في خدمات المنصات المشتركة. غالباً ما تحتوي صور الحاويات على شيفرة خاصة وبيانات اعتماد وبيانات تكوين. قد يؤدي التلاعب غير المصرح به بهذه المكونات إلى إدخال شيفرة خبيثة في بيئات الإنتاج أو كشف ملكية فكرية حساسة.

ينبغي للمؤسسات الخاضعة للتنظيم التي تعتمد على Docker Hub أو سجلات عامة مماثلة التحقق من عدم حدوث تعديلات غير مصرح بها خلال فترة الثغرة. يجب على المؤسسات أيضاً مراجعة ضوابط مصدر صور الحاويات والنظر فيما إذا كانت السجلات الخاصة أو آليات توقيع الصور الإضافية مبررة لأحمال العمل الحرجية.

حالة المعالجة

أكدت Docker تطبيق التصحيح في 30 سبتمبر وأن جميع مستخدمي Docker Hub محميون الآن. لا يلزم اتخاذ أي إجراء إضافي من مستخدمي المنصة نفسها، رغم أن المراجعات الأمنية اللاحقة تظل حكيمة للمؤسسات ذات الالتزامات التنظيمية بموجب أطر مثل الضوابط الأساسية للأمن السيبراني للهيئة الوطنية للأمن السيبراني أو إطار الأمن السيبراني لمؤسسة النقد العربي السعودي.

ما يجب فعله الآن

1. مراجعة سجلات نشر صور الحاويات من Docker Hub للفترة السابقة لـ 30 سبتمبر 2024 لتحديد أي نشاط شاذ في النشر أو السحب أو الحذف
2. التحقق من سلامة ومصدر جميع صور الحاويات الموجودة حالياً في الإنتاج والتي جُلبت من Docker Hub خلال فترة الثغرة
3. تقييم ما إذا كان الاعتماد الحالي على سجلات الحاويات العامة يتوافق مع قابلية المخاطر المؤسسية والنظر في الانتقال إلى سجلات خاصة لأحمال العمل الحساسة
4. تطبيق أو تعزيز ضوابط توقيع الصور والتحقق منها لاكتشاف التعديلات غير المصرح بها على مكونات الحاويات
5. تحديث تقييمات مخاطر سلسلة توريد البرمجيات لمراعاة ثغرات المصادقة في خدمات السجلات من جهات خارجية
6. إطلاع فرق التطوير وعمليات التطوير على الحادث وتعزيز ممارسات إدارة صور الحاويات الآمنة وفقاً

لمتطلبات الضوابط الأساسية للأمن السيبراني أو إطار الأمن السيبراني لساما