

ثغرتان حرجتان في MarkLogic تتيح التصعيد إلى صلاحيات المسؤول



كشفت Progress Software عن 31 ثغرة في خادم MarkLogic، بينها ثغرتان حرجتان تتيح للمديرين المفوضين الحصول على صلاحيات المسؤول بشكل دائم. صدرت التحديثات الأمنية في سبتمبر.

- كشفت Progress Software عن 31 ثغرة في خادم MarkLogic في 12 أكتوبر، خمس منها بدرجة حرجة
- تتيح ثغرتان حرجتان للحسابات ذات الصلاحيات الإدارية المحدودة التصعيد إلى صلاحيات المسؤول الكاملة
- التحديثات الأمنية متاحة منذ 10 سبتمبر في الإصدارين 11.3.7 و12.1.0
- تؤثر الثغرات على أنظمة قواعد البيانات التي قد تتعامل مع بيانات حساسة خاضعة للتنظيم

كشفت Progress Software عن 31 ثغرة أمنية في منصة خادم قاعدة البيانات MarkLogic، بما في ذلك ثغرتان

حرجتان تتيح **تصعيد الصلاحيات** من حسابات الإدارة المفوضة إلى السيطرة الكاملة بصلاحيات المسؤول. نشر المورد التنبيه الأمني في 12 أكتوبر، وصنّف خمساً من الثغرات بدرجة حرجة.

تفاصيل الثغرات

تتيح الثغرتان الأكثر خطورة لحسابات المستخدمين التي مُنحت صلاحيات إدارية محدودة تصعيد وصولها والحصول على سيطرة دائمة بمستوى المسؤول على خادم MarkLogic. يمثل هذا النوع من تصعيد الصلاحيات خطراً كبيراً على المؤسسات التي تعتمد على ضوابط الوصول القائمة على الأدوار لحماية البيانات الحساسة المخزنة في أنظمة قواعد البيانات.

التحديثات الأمنية متاحة منذ سبتمبر

أصدرت Progress Software تحديثات أمنية تعالج جميع الثغرات الـ 31 في 10 سبتمبر، قبل الإفصاح العلني. تتضمن الإصلاحات في إصدار MarkLogic 11.3.7 والإصدار 12.1.0. المؤسسات التي تشغل إصدارات أقدم تبقى معرضة للاستغلال المحتمل.

التداعيات على المؤسسات الخاضعة للتنظيم

بالنسبة للمؤسسات المالية ومقدمي الرعاية الصحية والجهات الأخرى الخاضعة للتنظيم في المملكة التي تستخدم خادم MarkLogic لإدارة البيانات، تشكل هذه الثغرات مخاطر على الامتثال والعمليات. غالباً ما تخزن أنظمة قواعد البيانات سجلات العملاء والمعاملات المالية وغيرها من المعلومات الحساسة الخاضعة لمتطلبات الحماية التنظيمية. قد يؤدي الوصول غير المصرح به بصلاحيات المسؤول إلى اختراقات البيانات أو تعديلات غير مصرح بها أو انتهاكات الامتثال بموجب الأطر المعمول بها.

ما يجب فعله الآن

1. حدد جميع خوادم MarkLogic في بيئتك وتحقق من أرقام الإصدارات الحالية مقابل التنبيه الأمني من المورد
2. أعط الأولوية للتحديث الفوري إلى الإصدار 11.3.7 أو 12.1.0 لجميع بيئات MarkLogic الإنتاجية وغير الإنتاجية
3. راجع سجلات التدقيق للكشف عن أي نشاط غير اعتيادي لتصعيد الصلاحيات أو إجراءات إدارية غير مصرح بها منذ سبتمبر
4. تحقق من صحة إعدادات ضوابط الوصول القائمة على الأدوار وقيد صلاحيات الإدارة المفوضة إلى الحد الأدنى الضروري
5. وثّق أنشطة التحديث وإصدارات البرمجيات كأدلة امتثال بموجب إطار الضوابط الأساسية للأمن السبيرياني وأطر ساما
6. نسّق مع مالكي التطبيقات لجدولة نوافذ الصيانة إذا تطلب التحديث انقطاع الخدمة