

جهات تهديد تستغل ثغرة حرجية في Collabora خوادم Nextcloud لاخترق



تستغل جهات مهاجمة الثغرة CVE-2026-110447 في تطبيق Collabora لـ Nextcloud لنشر أبواب خلفية والبحث عن بيانات اعتماد منذ منتصف سبتمبر.

- الثغرة CVE-2026-110447 تؤثر على إصدارات تطبيق Collabora Online Built-in CODE Server قبل 26.4.303 لـ Nextcloud
- بدأ الاستغلال النشط في منتصف سبتمبر قبل أكثر من أربعة أسابيع من نشر CVE في 14 أكتوبر
- ينشر المهاجمون أبواباً خلفية بلغة PHP للبحث عن قواعد بيانات كلمات المرور ومديري الكلمات والمحافظ الرقمية
- الثغرة لا تتطلب مصادقة وتستغل حقن أوامر في نقطة proxy.php عندما يكون الخادم متوقفاً
- فجوة 33 يوماً بين إصدار التصحيح في 11 سبتمبر ونشر CVE أعاققت استجابة المسؤولين

تفاصيل الثغرة والجدول الزمني للاستغلال

تستغل جهات تهديد بشكل نشط الثغرة CVE-2026-110447، وهي ثغرة حرجة لتنفيذ أوامر عن بُعد في تطبيق Nextcloud J Collabora Online Built-in CODE Server. تؤثر الثغرة على الإصدارات السابقة لـ 26.4.303 وتكمن في آلية التطبيق لبدء خادم Collabora المدمج. بدأ الاستغلال في منتصف سبتمبر، حيث وثقت تقارير المسؤولين هجمات في وقت مبكر من 10 سبتمبر.

تتيح الثغرة للمهاجمين حقن أوامر نظام التشغيل عبر نقطة proxy.php الخاصة بالتطبيق دون الحاجة إلى مصادقة أو تفاعل من المستخدم. الشرط الأساسي هو أن يكون خادم CODE المدمج متوقفاً، كما يحدث بعد إعادة تشغيل أو ترقية أو عطل. تؤثر الثغرة فقط على تطبيق خادم CODE المدمج الاختياري؛ بينما تبقى خوادم Collabora Online المستقلة وتثبيتات Docker والحزم ونشر Nextcloud All-in-One غير متأثرة.

أنماط الهجوم والتأخير في الإفصاح

أفاد المسؤولون بأن المهاجمين نشروا أبواباً خلفية بلغة PHP واستخدموها للبحث عن قواعد بيانات كلمات المرور ومخلفات مديري الكلمات والمحافظ الرقمية. أصدر المورد إصلاحاً في 9 سبتمبر وأطلق الإصدار 26.4.303 في 11 سبتمبر، لكن النشرة الرسمية ورقم CVE لم يُنشرا حتى 14 أكتوبر، مما خلق فجوة تزيد عن أربعة أسابيع. صدر تحذير من المجتمع في 3 أكتوبر يحث على التحديث الفوري بسبب الاستغلال المستمر، لكن غياب معرف CVE جعل من الصعب على المسؤولين تقييم المشكلة وتطبيق دفاعات.

الآثار الأوسع على إدارة الثغرات

وجد بحث من Second Security أن الفترة الوسيطة بين الإصلاحات العامة ونشر CVE ارتفعت إلى 39 يوماً في أغسطس، مقارنة بـ 5.1 أيام في يناير. يعزو الباحثون ذلك إلى تزايد أحجام اكتشافات الثغرات بمساعدة الذكاء الاصطناعي التي ترهق أنظمة معالجة CVE. في حالات كثيرة، ظهرت شيفرات استغلال عامة في غضون ساعات من الإصلاحات الأمنية وأيام قبل نشر CVE، حيث تمكّن أدوات الذكاء الاصطناعي المهاجمين من توليد استغلالات فعالة بسرعة من التصحيحات المنشورة.

ما يجب فعله الآن

1. الترقية الفورية لتطبيق richdocumentscode (Collabora Online Built-in CODE Server) إلى الإصدار 26.4.303 أو أحدث على جميع نسخ Nextcloud
2. إزالة تطبيق خادم CODE المدمج بالكامل إذا لم يكن مطلوباً للعمليات التشغيلية؛ التعطيل وحده غير كافٍ
3. إجراء مراجعة جنائية لجميع خوادم Nextcloud التي تشغل الإصدارات المتأثرة للبحث عن أبواب خلفية بلغة PHP، خاصة في الدلائل القابلة للوصول عبر الويب
4. البحث في سجلات النظام عن طلبات مشبوهة لنقاط proxy.php تعود إلى 10 سبتمبر
5. مراجعة سجلات الوصول للبحث عن أدلة على جمع بيانات الاعتماد أو استعلامات قواعد بيانات كلمات المرور أو عمليات بحث عن محافظ رقمية
6. تطبيق ضوابط تعويضية لمراقبة والتنبيه على محاولات تنفيذ الأوامر في دلائل تطبيقات الويب حتى اكتمال التصحيح