

اختراق خوادم Nextcloud وزرع أبواب خلفية عبر ثغرة في تطبيق Collabora CODE المدمج



استغل مهاجمون ثغرة حرجية في تطبيق Collabora Online - Built-in CODE Server الاختياري لزرع web shells على خوادم Nextcloud. أبلغ ثلاثة مديري أنظمة عنها عبر GitHub، وسُجِّل أول هجوم في 10 سبتمبر.

- المكوّن المتأثر هو التطبيق الاختياري Collabora Online - Built-in CODE Server وليس نواة Nextcloud.
- استخدم المهاجمون الثغرة لزرع web shells على خوادم Nextcloud.
- أبلغ ثلاثة مديري أنظمة عن المشكلة عبر GitHub.
- يعود أول هجوم مسجّل إلى 10 سبتمبر.
- تنقذ web shell أي أمر يرسله المهاجم عبر طلب ويب بصلاحيات حساب خادم الويب.

استغل مهاجمون ثغرة حرجة في تطبيق Nextcloud الاختياري Collabora Online - Built-in CODE Server لتثبيت web shells على خوادم Nextcloud. ووفق موقع The Hacker News، أبلغ ثلاثة مديري أنظمة عن المشكلة عبر GitHub، وسُجِّل أول هجوم في 10 سبتمبر.

أهمية الموضوع

ال web shell ملف صغير ينفَّذ أي أمر يرسله المهاجم عبر طلب ويب، بصلاحيات حساب خادم الويب. وبمجرد زرعه يحصل المهاجم على باب خلفي دائم قد يبقى حتى بعد إصلاح الثغرة الأصلية.

تقع المشكلة في تطبيق اختياري لا في نواة Nextcloud، لذا يُرجَّح أن تتأثر فقط الجهات التي تبتت خادم CODE المدمج وفعلته، ولا يتضمن المقطع المتاح تفاصيل تقنية إضافية ولا رقم CVE ولا معلومات عن التصحيح.

الخطوات التالية

على الجهات التي تشغِّل Nextcloud التأكد أولاً مما إذا كان هذا التطبيق مثبتاً. وإن كان كذلك، فليُعامل الخادم على أنه قد يكون مخترقاً إلى حين الفحص، وتُراجع نشرات المورّد وGitHub لمعرفة الإصدار المصحَّح، ويُبحث عن ملفات غير متوقعة في المجلدات المتاحة عبر الويب. ولأن المصدر لا يذكر إصلاحاً، ينبغي التحقق من حالة المعالجة مع المورّد مباشرة وعدم الاكتفاء بالتحديث.

ما يجب فعله الآن

1. التحقق مما إذا كان تطبيق Collabora Online - Built-in CODE Server مثبتاً ومفعّلاً على خوادم Nextcloud.
2. تعطيل التطبيق أو تقييده في حال وجوده إلى أن يؤكد المورّد توفر إصلاح.
3. فحص مجلدات الويب والتغييرات الحديثة على هذه الخوادم بحثاً عن ملفات مجهولة قد تكون web shells.
4. مراجعة سجلات خادم الويب بحثاً عن طلبات غير معتادة منذ 10 سبتمبر وحفظها للتحقيق.
5. عند الاشتباه بالاختراق: عزل الخادم وتغيير بيانات الاعتماد التي يصل إليها وتفعيل خطة الاستجابة للحوادث، مع إبلاغ الجهة التنظيمية المعنية عند الاقتضاء.