

ثغرة اجتياز المسار في ONLYOFFICE Docs تتيح تنفيذ التعليمات البرمجية عن بُعد



ثغرة اجتياز المسار في ONLYOFFICE Docs عند تفعيل مصادقة JWT تتيح للمهاجمين رفع صور ضارة وتنفيذ تعليمات برمجية عن بُعد على الخوادم المتأثرة.

- الثغرة CVE-2021-3199 تؤثر على ONLYOFFICE Docs Server عند استخدام مصادقة JWT
- يمكن للمهاجمين استغلال عيب اجتياز المسار عبر تسلسلات ../ في معاملات رفع الصور
- الاستغلال الناجح قد يؤدي إلى تنفيذ تعليمات برمجية عن بُعد على الخادم
- يجب على المؤسسات تطبيق تدابير المورّد أو إيقاف استخدام المنتج في حال عدم توفر التحديثات
- النسخة المعرّضة للإنترنت تتطلب تقييماً ومعالجة فورية

نظرة عامة على الثغرة

يحتوي ONLYOFFICE Docs Server على **ثغرة اجتياز المسار المتعقبة** برقم CVE-2021-3199 التي تؤثر على عمليات النشر التي تستخدم مصادقة JWT. تتيح هذه الثغرة للمهاجمين التلاعب بمعاملات رفع الصور من خلال إدراج تسلسلات /، متجاوزين بذلك قيود الدليل. تُنشئ هذه الثغرة مساراً لتنفيذ التعليمات البرمجية عن بُعد، مما يمكن المهاجمين من تشغيل أوامر عشوائية على الخادم المستضيف لمنصة التعاون على المستندات.

تستهدف الثغرة تحديداً وظيفة رفع الصور عند تكوين رموز JWT للمصادقة. يمكن للمهاجمين الذين يستغلون هذه الثغرة اجتياز بنية نظام الملفات، مما قد يتيح وضع ملفات ضارة في أدلة قابلة للتنفيذ أو الكتابة فوق ملفات النظام الحرجة.

المخاطر على المؤسسات السعودية

تواجه المؤسسات الخاضعة للتنظيم في المملكة التي تستخدم ONLYOFFICE Docs للتعاون على المستندات مخاطر كبيرة إذا كانت عمليات النشر لديها متاحة عبر الإنترنت ولم تطبق تدابير الموزد. يجب على المؤسسات المالية ومقدمي الرعاية الصحية والجهات الحكومية التي تتعامل مع بيانات حساسة عبر منصات المستندات التعاونية إعطاء الأولوية لتقييم ثغرات ONLYOFFICE لديها.

تعني قدرة تنفيذ التعليمات البرمجية عن بُعد أن المهاجمين قد يحصلون على سيطرة كاملة على الخوادم المتأثرة، مما قد يتيح الوصول إلى المستندات السرية أو بيانات العملاء أو استخدام الأنظمة المخترقة كنقاط ارتكاز لاختراق أوسع للشبكة.

إرشادات المعالجة

يجب على المؤسسات الرجوع فوراً إلى وثائق موزد ONLYOFFICE للحصول على التحديثات الأمنية المتاحة وتطبيقها وفقاً لإجراءات إدارة التغيير لديها. في حال عدم توفر التدابير أو عدم إمكانية تطبيقها بسرعة، ينبغي للمؤسسات النظر في عزل الأنظمة المتأثرة عن الوصول للإنترنت أو إيقاف الاستخدام حتى نشر التصديحات. تتطلب جميع نسخ ONLYOFFICE Docs المواجهة للإنترنت جرداً فورياً وتقييماً للمخاطر لتحديد مستويات التعرض وترتيب أولويات جهود المعالجة.

ما يجب فعله الآن

1. تحديد جميع عمليات نشر ONLYOFFICE Docs Server في بيئتك، خاصة تلك التي تستخدم مصادقة JWT
2. تقييم تعرض كل نسخة من ONLYOFFICE للإنترنت وتوثيق إمكانية الوصول الخارجي
3. الرجوع إلى نشرات الأمان من موزد ONLYOFFICE للحصول على التصديحات وتطبيق التحديثات عبر عملية إدارة التغيير
4. في حال عدم إمكانية التصحيح الفوري، عزل الأنظمة المتأثرة عن الوصول للإنترنت أو تطبيق ضوابط وصول على مستوى الشبكة
5. مراجعة سجلات الوصول للكشف عن نشاط رفع صور مشبوه أو أنماط غير عادية لاجتياز نظام الملفات
6. النظر في إيقاف استخدام ONLYOFFICE Docs إذا لم تكن تدابير الموزد متاحة ولا يمكن احتواء المخاطر

