مايكروسوفت تدرج الثغرة CVE-2026-97761 للتنفيذ عن بُعد في Microsoft Office Excel



أدرجت مايكروسوفت في دليل التحديثات الثغرة CVE-2026-97761 للتنفيذ عن بُعد في Excel. والمراجعة الأخيرة اقتصرت على تحديث إشادة دون أي تغيير تقني.

- الإدراج بعنوان ثغرة تنفيذ تعليمات برمجية عن بُعد في Microsoft Office Excel ويحمل المعرّف CVE-2026-97761.
- التحديث الأخير عدّل إشادة فقط، وتصفه مايكروسوفت بأنه تغيير معلوماتي.
- المقتطف المتاح لا يتضمن درجة الخطورة أو الإصدارات المتأثرة أو حالة الاستغلال أو تفاصيل التصحيح.

نشرت مايكروسوفت في دليل التحديثات الأمنية إدراجًا للثغرة CVE-2026-97761، وهي ثغرة تنفيذ تعليمات برمجية عن بُعد في Microsoft Office Excel.

ما تقوله المصدر

التغيير الوحيد المذكور في المراجعة الأخيرة هو تحديث إشادة. وتؤكد مايكروسوفت أن التغيير معلوماتي فقط، أي أنه لا يعدّل المحتوى التقني للإدراج ولا يستدعي إجراءً جديدًا بحد ذاته.

المقتطف المتاح لنا لا يتضمن درجة الخطورة، ولا قائمة إصدارات Office المتأثرة، ولا ما إذا كانت الثغرة مستغَلة، ولا التصحيح نفسه. لذلك لم نفترض شيئًا بشأن هذه النقاط.

الخطوة التالية

على الفرق التي تستخدم Excel فتح الإدراج الكامل في دليل التحديثات الأمنية لدى مايكروسوفت، وقراءة المنتجات المتأثرة ودرجة الخطورة وتفاصيل المعالجة، فهي ما يحدد سرعة نشر التصحيح.

ينبغي للمنظمات التحقق مما إذا كان التحديث مشمولاً بدورة تحديث Office المعتادة لديها، والتأكد من أن سجلات الأصول توضح إصدارات Excel المستخدمة. وإذا أكد الإدراج توفر إصلاح، فيُجدول وفق سياسة إدارة الثغرات الداخلية ويُوثَّق القرار لأغراض التدقيق.

إلى حين مراجعة التفاصيل الكاملة، لا يوجد في المصدر ما يبرر إجراءات طارئة. ويستمر تطبيق الضوابط المعتادة على الملفات الواردة من خارج المنظمة.

ما يجب فعله الآن

1. فتح إدراج CVE-2026-97761 الكامل في دليل التحديثات الأمنية لدى مايكروسوفت وتدوين الإصدارات المتأثرة ودرجة الخطورة والإصلاح.
2. تحديد إصدارات Excel وOffice المنتشرة على الأجهزة الطرفية.
3. التأكد من أن الإصلاح مشمول بدورة تحديث Office المعتادة وجدولته وفق سياسة إدارة الثغرات.
4. توثيق التقييم والقرار لأغراض التدقيق ومراجعة الجهات التنظيمية.