مايكروسوفت تدرج ثغرة تنفيذ التعليمات البرمجية عن بُعد في Excel برقم CVE-2026-118302



نشرت مايكروسوفت الثغرة CVE-2026-118302 وهي ثغرة تنفيذ تعليمات برمجية عن بُعد في Microsoft Office Excel. التحديث الأخير يعدّل إقرارًا فقط، ولا يتضمن المقتطف درجة الخطورة أو تفاصيل الإصلاح.

- تُتابَع الثغرة تحت الرقم CVE-2026-118302 وتخص Microsoft Office Excel.
- صُنّفت على أنها ثغرة تنفيذ تعليمات برمجية عن بُعد.
- آخر تعديل شمل تحديث إقرار فقط وهو تغيير معلوماتي.
- لا يتضمن المقتطف درجة الخطورة أو الإصدارات المتأثرة أو تفاصيل التصحيح.

تتضمن بوابة Microsoft Security Response Center سجلاً للثغرة CVE-2026-118302، ووصفتها بأنها ثغرة تنفيذ تعليمات برمجية عن بُعد في Microsoft Office Excel.

ما ورد في المصدر

يحدد السجل المنتج المتأثر (Microsoft Office Excel) ونوع الثغرة (تنفيذ تعليمات برمجية عن بُعد). وقد شمل آخر تعديل تحديث إقرار، وتصفه مايكروسوفت بأنه تغيير معلوماتي فقط، أي أنه لا يشير إلى تغيّر في طبيعة المشكلة.

لا يتضمن المقتطف الذي راجعناه درجة الخطورة ولا الإصدارات المتأثرة ولا حالة الاستغلال ولا خطوات المعالجة، ولذلك لا نذكر شيئًا عن هذه النقاط.

الأثر على المؤسسات

يُستخدم Excel على نطاق واسع في القطاع المالي والجهات الحكومية والأعمال، ما يجعل أي ثغرة تنفيذ عن بُعد فيه جديرة بفحص سريع لبيئتكم. والخطوة العملية هي قراءة الإشعار الكامل في Microsoft Update Guide، والتحقق مما إذا كانت إصدارات Office لديكم مدرجة، واتباع إرشادات الشركة بشأن التحديثات.

ولأن تعديل الإقرار لا يحمل أثرًا تقنيًا، فلا حاجة لإعادة التقييم لدى الفرق التي قيّمت هذه الثغرة سابقًا. أما الفرق التي لم تفعل، فينبغي إدراجها في قائمة فرز التحديثات المعتادة وتحديد أولويتها وفق الخطورة وتفاصيل الاستغلال التي تنشرها مايكروسوفت.

ما يجب فعله الآن

1. الاطلاع على سجل CVE-2026-118302 كاملاً في Microsoft Update Guide.
2. مراجعة سجل الأصول لتحديد تثبيتات Microsoft Office Excel وإصداراتها.
3. تطبيق التحديث أو إجراء التخفيف الذي تنشره مايكروسوفت بعد التأكد من انطباقه على إصداراتكم.
4. إدراج الثغرة في متابعة إدارة التحديثات بأولوية مبنية على بيانات الخطورة من مايكروسوفت.
5. تذكير المستخدمين بالحذر من ملفات الجداول غير المتوقعة إلى حين اكتمال التحديث.