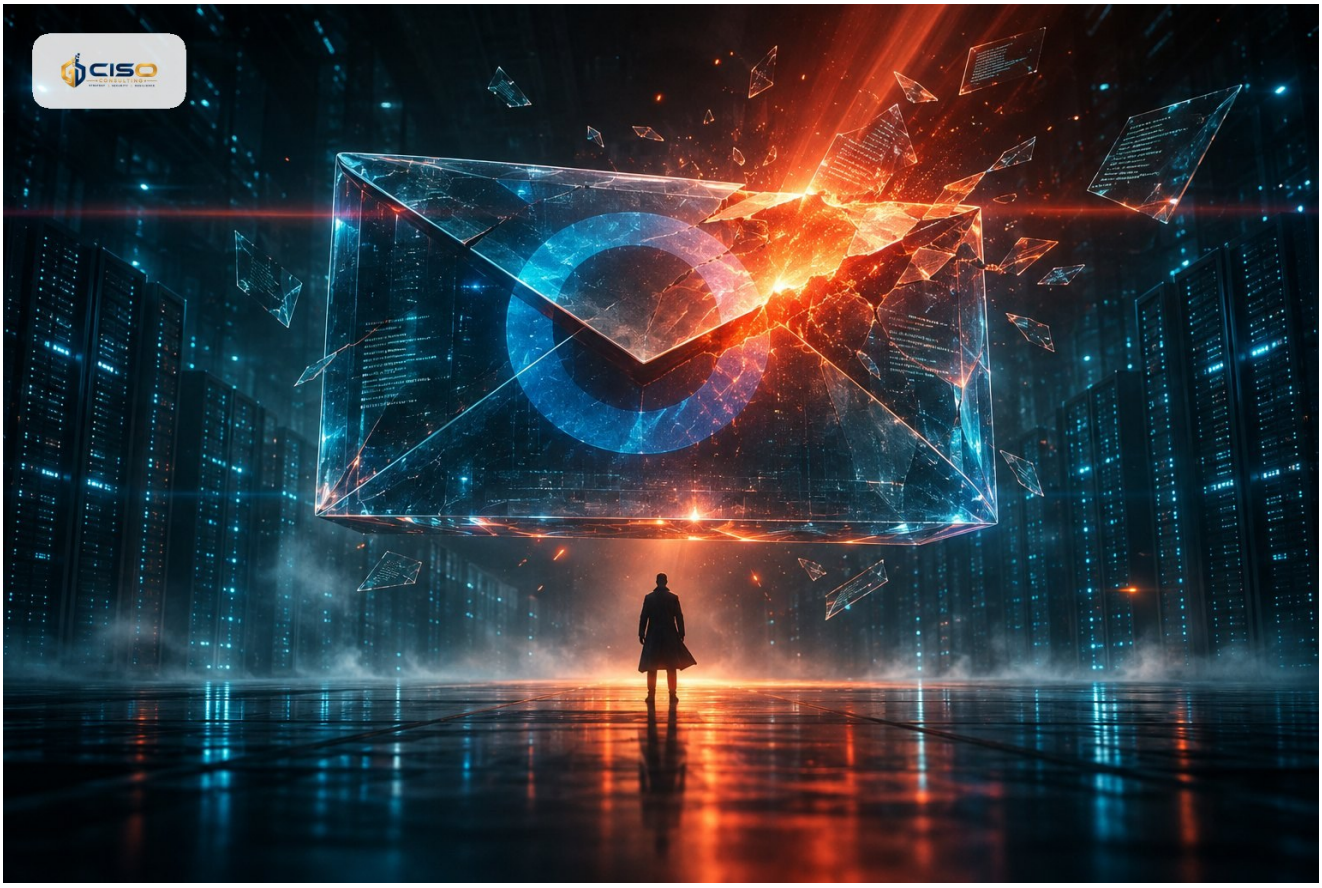
مايكروسوفت تدرج الثغرة CVE-2026-97749 في Outlook للتنفيذ عن بُعد



نشرت مايكروسوفت الثغرة CVE-2026-97749 في Microsoft Office Outlook، وهي تتيح تنفيذ التعليمات البرمجية عن بُعد. وتحديث السجل الأخير يخص إشادة فقط وهو معلوماتي.

- السجل بعنوان Microsoft Office Outlook Remote Code Execution Vulnerability ويحمل المعرّف CVE-2026-97749.
- نُشر في دليل التحديثات الأمنية لدى مايكروسوفت (MSRC).
- التحديث الأخير عدّل إشادة فقط، وتصفه مايكروسوفت بأنه تغيير معلوماتي.
- المقتطف المتاح لا يذكر درجة الخطورة ولا الإصدارات المتأثرة ولا حالة الاستغلال.

يتضمن دليل التحديثات الأمنية من مايكروسوفت الثغرة CVE-2026-97749، وهي ثغرة تنفيذ تعليمات برمجية عن بُعد تؤثر في Microsoft Office Outlook.

ما الذي يذكره المصدر

يصنّف السجل المشكلة على أنها ثغرة تنفيذ تعليمات برمجية عن بُعد في Outlook. وقد عدّل التحديث الأخير إشادة، وتوضح مايكروسوفت أن هذا تغيير معلوماتي فقط، أي أنه لا يشير إلى تغيير في المحتوى التقني للنشرة.

لا يتضمن المقتطف المتاح لنا درجة الخطورة ولا قائمة الإصدارات المتأثرة ولا شروط الهجوم ولا توفر الإصلاح ولا أي إشارة إلى استغلال الثغرة. ولذلك لم نفترض شيئًا بشأن هذه النقاط.

ما يعنيه ذلك لمنشأتكم

يُستخدم Outlook على نطاق واسع في الجهات المنظَّمة، لذا يستحق أي سجل لتنفيذ التعليمات عن بُعد مراجعة سريعة مقابل بيئتكم. والخطوة العملية هي قراءة السجل الكامل في دليل التحديثات الأمنية، والتحقق من إدراج إصدارات Outlook لديكم، ثم تطبيق إرشادات المعالجة من مايكروسوفت عبر إجراءات التحديث المعتادة.

ولأن التحديث الأخير معلوماتي، فلا حاجة لإعادة التقييم لدى الفرق التي راجعت هذه الثغرة سابقًا. أما من لم يفعل، فعليه إدراج المراجعة ضمن إدارة الثغرات الدورية وتحديد أولويتها وفق التفاصيل في السجل الرسمي.

ما يجب فعله الآن

1. افتحوا سجل CVE-2026-97749 في دليل التحديثات الأمنية من مايكروسوفت واقرأوا الإصدارات المتأثرة وإرشادات المعالجة.
2. راجعوا سجل الأصول لديكم لتحديد إصدارات Outlook المنشورة.
3. طبّقوا إصلاح المورّد عبر إدارة التحديثات المعتمدة مع ترتيب الأولوية بحسب تفاصيل الخطورة في السجل.
4. وثّقوا المراجعة والقرار المتخذ في سجل إدارة الثغرات لأغراض التدقيق.