مايكروسوفت تُدرج الثغرة CVE-2026-69918 في مكوّن Windows Core Messaging لرفع الصلاحيات



يُدرج دليل تحديثات مايكروسوفت الثغرة CVE-2026-69918، وهي ثغرة رفع صلاحيات في Windows Core Messaging. وآخر تعديل اقتصر على تحديث إشادة دون تغيير تقني.

- تُتابَع الثغرة تحت الرقم CVE-2026-69918.
- صُنّفت كثغرة رفع صلاحيات في مكوّن Windows Core Messaging.
- التعديل الأخير حدّث إشادة فقط، ووُصف بأنه معلوماتي.
- لا يتضمن المقتطف درجة خطورة أو حالة استغلال أو الإصدارات المتأثرة.

نشر مركز الاستجابة الأمنية في مايكروسوفت مدخلًا للثغرة CVE-2026-69918، ووصفها بأنها ثغرة رفع صلاحيات في مكوّن Windows Core Messaging.

ما ورد في المصدر

جرى تعديل المدخل لتحديث إشادة، وتذكر مايكروسوفت أن التغيير معلوماتي فقط. ولذلك لا يغيّر هذا التعديل المحتوى التقني للنشرة ولا يعني صدور توجيه جديد.

لا يتضمن النص المتاح لنا درجة الخطورة، ولا كيفية استغلال الثغرة، ولا ما إذا كانت مستغلة فعلًا، ولا إصدارات Windows المتأثرة. لذا لا نقدّم أي ادعاءات بشأن هذه النقاط.

الأثر على المنشأة

تكتسب ثغرات رفع الصلاحيات أهميتها عادةً لأنها قد تتيح لمن يملك وصولًا محدوداً الحصول على صلاحيات أوسع على النظام. وعملياً، ينبغي للجهات المنظَّمة التعامل مع المدخل بوصفه بنداً ضمن إدارة التصحيحات، والتحقق من تفاصيله مباشرة لدى مايكروسوفت.

ويبقى المدخل الكامل في دليل تحديثات مايكروسوفت المرجع المعتمد لمعرفة المنتجات المتأثرة والتحديثات المتاحة وأي إجراءات تخفيف قبل تحديد الأولوية والتوقيت.

ما يجب فعله الآن

1. افتح مدخل CVE-2026-69918 في دليل تحديثات مايكروسوفت ودوّن إصدارات Windows المتأثرة والتحديثات المتاحة.
2. راجع سجل الأصول لتحديد أنظمة Windows التي قد تقع ضمن النطاق.
3. أضف البند إلى قائمة إدارة التصحيحات وحدّد أولويته بعد تأكيد تفاصيل الخطورة لدى مايكروسوفت.
4. اختبر التحديث المعني في بيئة تجريبية قبل نشره على نطاق أوسع وفق إجراءات إدارة التغيير.
5. راجع صلاحيات الإدارة المحلية على أجهزة وخوادم Windows كإجراء تحصين عام.