مايكروسوفت تدرج الثغرة CVE-2026-113817 المتعلقة برفع الصلاحيات في مكوّن Windows Devices Human Interface



أدرج دليل تحديثات مايكروسوفت الثغرة CVE-2026-113817 وهي ثغرة رفع صلاحيات في Windows Devices Human Interface. التعديل الأخير اقتصر على تحديث إشادة، دون تفاصيل إضافية.

- الثغرة CVE-2026-113817 هي ثغرة رفع صلاحيات في Windows Devices Human Interface.
- المصدر هو دليل التحديثات الصادر عن مركز MSRC التابع لمايكروسوفت.
- التعديل الأخير حدّث إشادة فقط ووُصف بأنه معلوماتي.
- المقتطف لا يتضمن درجة الخطورة أو الإصدارات المتأثرة أو حالة الاستغلال.

ما ورد في المصدر

يدرج مركز الاستجابة الأمنية لدى مايكروسوفت (MSRC) الثغرة CVE-2026-113817 بوصفها ثغرة رفع صلاحيات تؤثر في مكوّن Windows Devices Human Interface. وقد حدّث آخر تعديل على الإدخال إشادة، ووصفته مايكروسوفت بأنه تغيير معلوماتي فقط.

ما لم يذكره المصدر

لا يتضمن النص المتاح تصنيفًا للخطورة ولا درجة CVSS ولا قائمة بإصدارات Windows المتأثرة ولا توفر إصلاح ولا ما إذا كانت الثغرة مستغلة فعليًا. لذلك لم نمنحها مستوى خطورة يتجاوز ما يدعمه المصدر، ولم نستنتج تفاصيل من اسم المكوّن.

كيفية التعامل معها

تكمن أهمية ثغرات رفع الصلاحيات عادةً في أنها قد تتيح لمستخدم أو عملية محدودة الصلاحيات الحصول على صلاحيات أعلى على النظام. وانطباق ذلك هنا يعتمد على تفاصيل الإدخال الكامل لدى مايكروسوفت، وينبغي لفرق الأمن الاطلاع عليه مباشرة.

ولأن التعديل الأخير معلوماتي، فهو لا يشير بحد ذاته إلى تغيير في الاستجابة المطلوبة. والخطوة العملية هي التحقق من انطباق الإدخال على بيئة Windows لديكم، ومعالجته عبر إجراءات إدارة التحديثات والثغرات المعتمدة بعد مراجعة إرشادات مايكروسوفت.

ما يجب فعله الآن

1. مراجعة الإدخال الكامل للثغرة CVE-2026-113817 في دليل تحديثات مايكروسوفت لمعرفة الإصدارات المتأثرة وتفاصيل الإصلاح.
2. مطابقة سجل الأصول لتحديد أنظمة Windows التي قد تكون ضمن النطاق.
3. معالجة البند عبر إجراءات إدارة التحديثات والثغرات المعتمدة فور التأكد من توفر الإصلاح.
4. توثيق نتيجة المراجعة ضمن تقارير إدارة الثغرات.