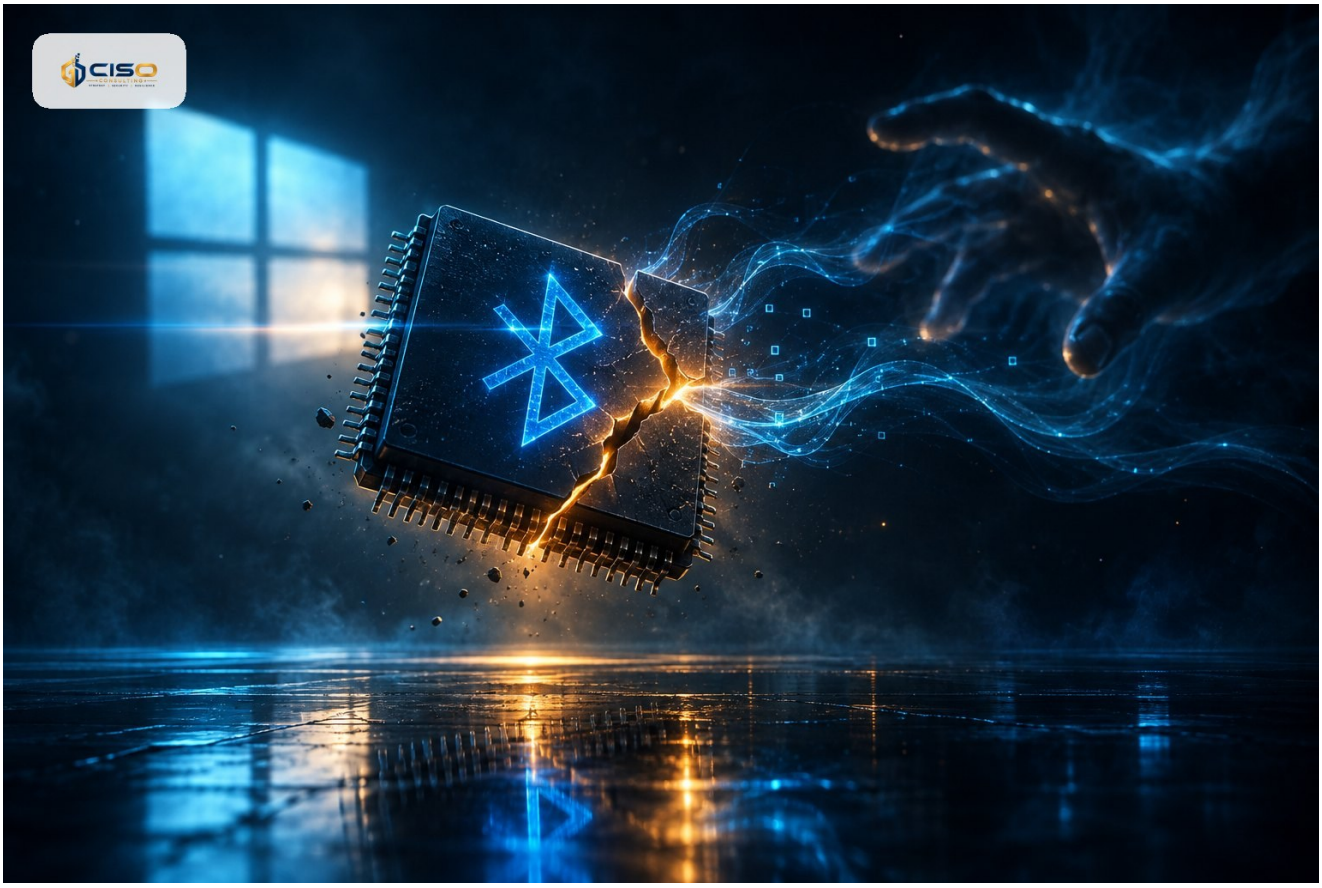
مايكروسوفت تدرج الثغرة CVE-2026-83760 في برنامج تشغيل البلوتوث وتتيح الإفصاح عن المعلومات



نشرت مايكروسوفت الثغرة CVE-2026-83760 وهي ثغرة إفصاح عن المعلومات في برنامج تشغيل البلوتوث. التحديث الأخير يقتصر على تعديل في الشكر والتقدير ولا يغيّر المحتوى التقني.

- تتابع مايكروسوفت الثغرة تحت الرقم CVE-2026-83760 في دليل التحديثات الأمنية.
- صُنفت على أنها ثغرة إفصاح عن المعلومات في برنامج تشغيل البلوتوث من مايكروسوفت.
- التعديل الأخير يخص عبارة شكر وتقدير ووصفته مايكروسوفت بأنه تغيير معلوماتي فقط.
- المقتطف المتاح لا يتضمن درجة الخطورة ولا الإصدارات المتأثرة ولا تفاصيل عن الاستغلال.

ما الذي نُشر

يدرج دليل التحديثات الأمنية من مايكروسوفت الثغرة CVE-2026-83760 ويصفها بأنها ثغرة إفصاح عن المعلومات

في برنامج تشغيل البلوتوث (Microsoft Bluetooth Driver). وقد تناول آخر تعديل على الإدخال عبارة شكر وتقدير، وأوضحت مايكروسوفت أنه تغيير معلوماتي فقط.

ما لا تذكره المصدر

لا يتضمن المقتطف المتاح درجة الخطورة، ولا إصدارات Windows المتأثرة، ولا الشروط اللازمة لاستغلال الثغرة، ولا ما إذا كانت مستغلة فعلياً. ينبغي الرجوع إلى إدخال مايكروسوفت مباشرة لمعرفة هذه التفاصيل قبل اتخاذ أي قرار يخص المخاطر. ولم نضف أي افتراضات تتجاوز ما ذكرته الجهة المصنِّعة.

الدلالات العملية

بما أن هذا التعديل لا يغيّر المحتوى التقني، فلا يستدعي بذاته أعمال طوارئ جديدة. لكنه فرصة مناسبة للتأكد من أن أجهزة Windows مشمولة بدورة التحديثات المعتادة، ومن مراجعة إدخال مايكروسوفت بحثاً عن التحديثات المنطبقة.

يمكن للفرق التي تحتفظ بسجل للثغرات تسجيل هذا الرقم، وتوثيق أن التعديل معلوماتي، وتكليف مسؤول بمراجعة الإشعار الكامل لمعرفة المنتجات المتأثرة والتحديثات المتاحة.

ما يجب فعله الآن

1. سجّلوا CVE-2026-83760 في سجل الثغرات مع الإشارة إلى أن آخر تعديل معلوماتي.
2. راجعوا إدخال مايكروسوفت الكامل للتأكد من إصدارات Windows المتأثرة والتحديثات الأمنية المتاحة.
3. تأكدوا من أن أجهزة Windows التي يتوفر فيها البلوتوث مشمولة بدورة التحديث المعتادة.
4. إن لم تكن هناك حاجة للبلوتوث على الأجهزة المُدارة، فراجعوا إمكانية تعطيله ضمن خط الأساس للإعدادات.