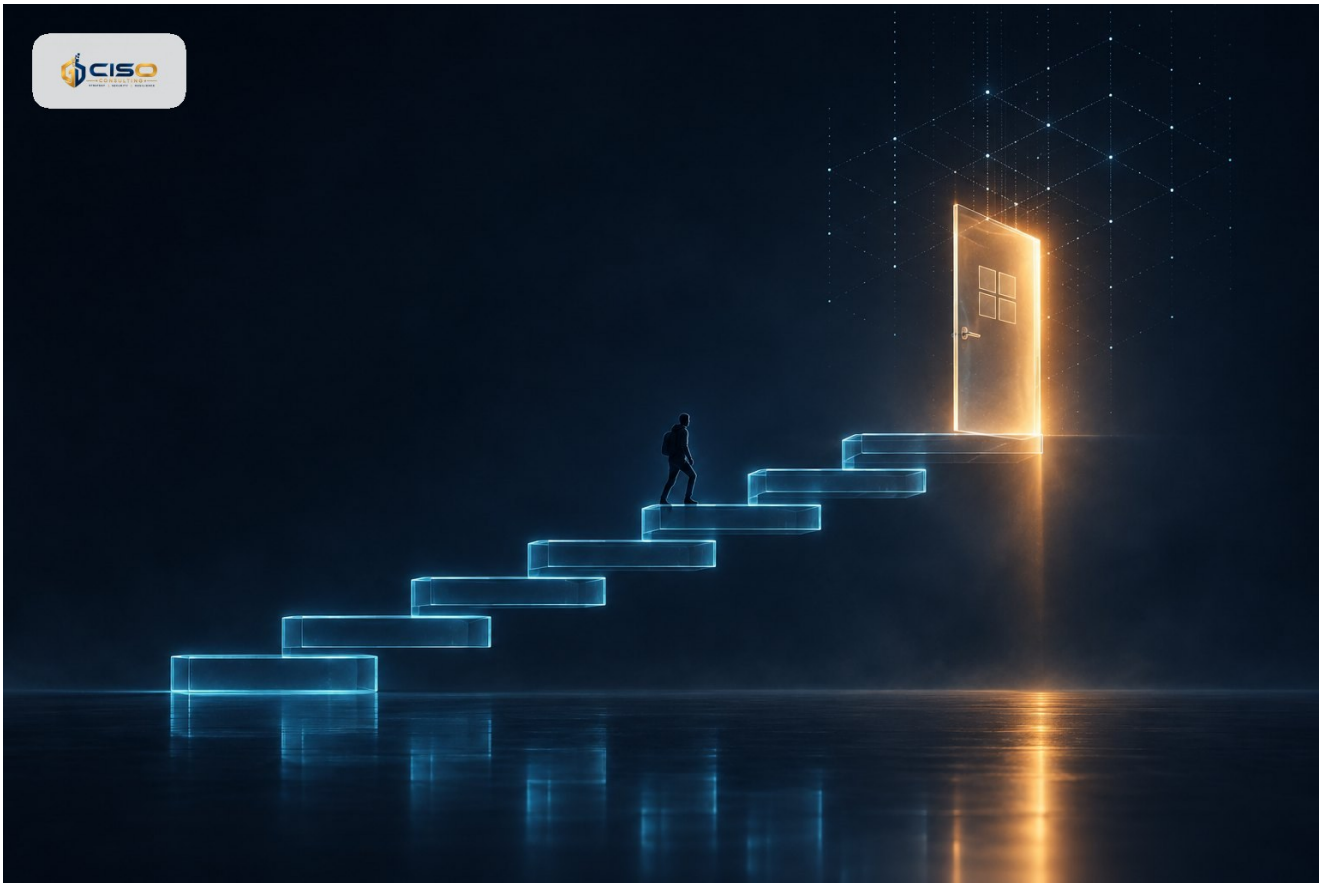
مايكروسوفت تدرج الثغرة CVE-2026-109481 في ASP.NET Core لرفع الصلاحيات



نشر مركز MSRC من مايكروسوفت إدخالًا للثغرة CVE-2026-109481 في ASP.NET Core لرفع الصلاحيات. والتحديث الأخير يقتصر على تعديل إشادة وهو معلوماتي فقط.

- الثغرة مسجلة بالرقم CVE-2026-109481 وتخص ASP.NET Core.
- تصنفها مايكروسوفت ثغرة رفع صلاحيات.
- التحديث الأخير يعدّل إشادة فقط ووصفته مايكروسوفت بأنه معلوماتي.
- لا يتضمن المقتطف المتاح درجة الخطورة ولا الإصدارات المتأثرة ولا تفاصيل التصحيح.

ما الذي نُشر

يُدرج مركز مايكروسوفت للاستجابة الأمنية (MSRC) في دليل التحديثات الثغرة CVE-2026-109481 بوصفها ثغرة

رفع صلاحيات في ASP.NET Core. وقد اقتصر آخر تعديل على الإدخال على تحديث إشادة، ووصفته مايكروسوفت بأنه تغيير معلوماتي، أي أنه لا يعني تغيراً في التقييم الفني.

ما لا يذكره المصدر

لا تتضمن المادة المتاحة لنا درجة الخطورة، ولا الإصدارات المتأثرة، ولا شروط الاستغلال، ولا ما إذا رُصد استغلال فعلي، كما لا تصف الإصلاح. لذلك لا نستخلص حكماً على المخاطر، ونوصي بالاطلاع على إدخال MSRC الكامل مباشرة.

الأثر على جهتكم

تكمن أهمية ثغرات رفع الصلاحيات في أنها قد تتيح لحساب أو عملية الحصول على وصول يتجاوز المقصود. وعلى الجهات التي تشغّل تطبيقات ويب أو واجهات برمجية على ASP.NET Core أن تتحقق من وجودها ضمن النطاق المتأثر وأن تراجع إرشادات المورّد. وهذا فحص روتيني لا حالة طارئة ما لم يشر الإدخال الكامل إلى خلاف ذلك.

وبالنسبة للجهات الخاضعة للتنظيم، يمثل الخبر فرصة للتأكد من أن إدارة الثغرات والتحديثات لديها تشمل نشرات المورّدين لأطر تطوير التطبيقات، وليس أنظمة التشغيل والأجهزة الشبكية فقط.

ما يجب فعله الآن

1. راجعوا سجل التطبيقات لديكم لتحديد أحمال ASP.NET Core، بما فيها التطبيقات المطوّرة داخلياً وتطبيقات الأطراف الثالثة.
2. اقرؤوا إدخال MSRC الكامل للثغرة CVE-2026-109481 للتأكد من الإصدارات المتأثرة والتحديث المتاح.
3. جدولوا أي تحديث مطلوب عبر إدارة التغيير والتحديثات المعتادة مع ترتيب الأولوية بحسب مستوى التعرض.
4. وثّقوا نتيجة المراجعة كدليل على ضوابط إدارة الثغرات.