ثغرة حرجة في مكتبة Idunno.AntiCsrf القديمة لـ ASP.NET يجري استغلالها فعلياً



يدعو باحثون إلى التوقف عن استخدام مكتبة Idunno.AntiCsrf القديمة بعد اكتشاف ثغرة حرجة CVE-2026-131914 بدرجة 9.3 جرى استغلالها فعلياً. وتشمل الإصدارين 0.9.1.0 و0.9.1 Beta.

- المكوّن المتأثر هو مكتبة Idunno.AntiCsrf (الملف Idunno.AntiCsrf.dll) القديمة للحماية من CSRF في ASP.NET.
- تحمل الثغرة المعرّف CVE-2026-131914 ودرجة 9.3 من 10.0 وفق CVSS.
- الإصداران المتأثران هما 0.9.1.0 و0.9.1 Beta.
- رُصد استغلال الثغرة فعلياً.
- يصف عنوان الخبر الأثر بأنه تنفيذ أوامر عن بُعد دون مصادقة، وينصح الباحثون بالتوقف عن استخدام المكتبة.

نصح باحثون المؤسسات بالتوقف عن استخدام Idunno.AntiCsrf، وهي مكتبة قديمة للحماية من هجمات CSRF في ASP.NET، بعد اكتشاف ثغرة حرجة فيها جرى استغلالها فعلياً.

ما المعروف حتى الآن

تحمل الثغرة المعرّف CVE-2026-131914 ودرجة 9.3 من 10.0 وفق مقياس CVSS. وتمس الإصدارين 0.9.1.0 و0.9.1 Beta من المكتبة التي تأتي في الملف Idunno.AntiCsrf.dll. ويصف عنوان التقرير الأثر بأنه تنفيذ أوامر عن بُعد دون مصادقة. أما المقتطف المتاح لدينا فلا يوضح الآلية التقنية ولا طبيعة الاستغلال ولا وجود إصدار مُصحَّح، ولذلك ينبغي التحقق من هذه النقاط في التقرير الكامل وتوجيهات الجهة المطوِّرة.

أهمية الأمر

تقع مكتبات الحماية من CSRF ضمن مسار الطلبات في تطبيقات الويب، وقد تظل تطبيقات ASP.NET القديمة تعتمد على هذه المكتبة دون أن يكون ذلك معروفاً على نطاق واسع. ومع ثغرة حرجة مستغلة فعلًا ولا تتطلب مصادقة، تزداد أولوية حصر كل التطبيقات التي تستخدمها، سواء الداخلية أو المقدَّمة من موردين.

الخطوات التالية

ابدأوا بالحصر ثم قرروا بين الإزالة والاستبدال. وبما أن الباحثين يوصون بالتوقف عن استخدام المكتبة وليس بتحديثها فحسب، فينبغي التخطيط للانتقال إلى بديل مدعوم.

ما يجب فعله الآن

1. البحث في شيفرة التطبيقات وملفات البناء والخوادم عن Idunno.AntiCsrf.dll وتحديد الإصدارين 0.9.1.0 و0.9.1 Beta.
2. سؤال الموردين وفرق التطوير الداخلية عمّا إذا كانت تطبيقات ASP.NET لديهم تستخدم المكتبة.
3. التخطيط لإزالة المكتبة أو استبدالها بآلية حماية من CSRF مدعومة، ومراجعة توجيهات الجهة المطوِّرة بشأن أي إصلاح.
4. مراجعة سجلات خوادم الويب والتطبيقات على الأنظمة المتأثرة بحثاً عن نشاط مشبوه، والتصعيد عبر مسار الاستجابة للحوادث عند وجوده.
5. تسجيل النتيجة في سجلات الثغرات والمكونات البرمجية لدى الأطراف الثالثة، ورفع أي تعرّض جوهري وفق إجراءات التصعيد الداخلية.