CISA تحذّر من ثغرة إلغاء تسلسل في Idunno AntiCsrf تتيح تنفيذ التعليمات عن بُعد (CVE-2026-131914)



أدرجت CISA الثغرة CVE-2026-131914 في Idunno AntiCsrf، وهي تتيح لمهاجم عن بُعد دون مصادقة تنفيذ تعليمات برمجية. وقد يكون المنتج منتهي الدعم، ويُنصح بتطبيق إجراءات المورّد أو التوقف عن استخدامه.

- CVE-2026-131914 ثغرة إلغاء تسلسل لبيانات غير موثوقة في Idunno AntiCsrf.
- يمكن لمهاجم عن بُعد دون مصادقة تنفيذ تعليمات برمجية عبر حقن الكائنات.
- قد يكون المنتج المتأثر منتهي الدعم أو الخدمة.
- يُنصح المستخدمون بالتوقف عن استخدامه أو الانتقال إلى إصدار مدعوم.
- الموعد النهائي لدى الجهات الفيدرالية الأمريكية هو 27-11-2026، ويقع على عاتق الجهات تقييم تعرّض كل أصل للإنترنت.

ما الذي أُعلن

أدرجت CISA الثغرة CVE-2026-131914 في Idunno AntiCsrf، وهي ثغرة إلغاء تسلسل لبيانات غير موثوقة. ووفق الإدراج، يستطيع مهاجم عن بُعد ودون مصادقة تنفيذ تعليمات برمجية عبر حقن الكائنات. وغياب شرط المصادقة هو ما يجعل الثغرة بالغة الأهمية لأي تطبيق مكشوف.

كما يشير الإدراج إلى أن المنتج المتأثر قد يكون منتهي الدعم أو الخدمة. وفي هذه الحالة يُنصح المستخدمون بالتوقف عن استخدامه أو الانتقال إلى إصدار مدعوم.

ما تطلبه CISA

الإجراء المطلوب هو تطبيق إجراءات التخفيف وفق تعليمات المورّد، مع الالتزام بتوجيه CISA رقم BOD 26-04 بشأن ترتيب أولوية التحديثات الأمنية بحسب المخاطر، ومتطلبات الفرز الجنائي (Forensics Triage Requirements). وبالنسبة للخدمات السحابية يُتّبع توجيه BOD 26-04 المعني بها. وإذا لم تتوفر إجراءات تخفيف فيجب التوقف عن استخدام المنتج. وتتحمل الجهات مسؤولية تقييم تعرّض كل أصل للإنترنت. والموعد النهائي للجهات الفيدرالية الأمريكية هو 27-11-2026.

القراءة العملية للمؤسسات في المملكة

يسري التوجيه والموعد على الجهات الفيدرالية الأمريكية، لكن منطقه يصلح لغيرها. ينبغي أولاً التحقق مما إذا كان أي تطبيق أو مكوّن لدى المؤسسة يتضمن Idunno AntiCsrf، ثم تقدير مدى تعرّض هذه الأنظمة للإنترنت. وإذا تعذّر التخفيف أو كان المكوّن غير مدعوم فينبغي التخطيط لاستبداله. ولا يذكر المصدر استغلالاً فعليًا للثغرة ولا إصدارات مصحَّحة، لذا يُرجى التأكد من التفاصيل لدى المورّد.

ما يجب فعله الآن

1. حصر التطبيقات والمكونات الخارجية لمعرفة أي استخدام لـ Idunno AntiCsrf.
2. تحديد الأصول المتأثرة المكشوفة للإنترنت ومعالجتها أولاً.
3. تطبيق إجراءات التخفيف من المورّد، أو التخطيط للانتقال إلى إصدار مدعوم إذا كان المنتج منتهي الدعم.
4. التوقف عن استخدام المنتج عند عدم توفر أي إجراء تخفيف.
5. مراجعة السجلات وحفظ الأدلة على الأنظمة المكشوفة للتحقق من أي مؤشرات اختراق.