استغلال ثغرة غير مصححة في مكتبة Idunno AntiCsrf (CVE-2026-131914) لتنفيذ أوامر عن بُعد



يستغل مهاجمون الثغرة (CVSS 9.3) CVE-2026-131914 في وحدة Idunno AntiCsrf المهجورة لتطبيقات ASP.NET WebForms. لا يوجد تصحيح ولا يُتوقع صدوره، ويُنصح باستبدال المكتبة.

- الثغرة (CVSS 9.3) CVE-2026-131914 هي خلل في إلغاء التسلسل غير الآمن عند معالجة طلبات HTTP POST الموجهة إلى نقاط ASP.NET WebForms.
- يكفي طلب POST واحد دون مصادقة ودون رمز CSRF صالح، وقد رصدت Mandiant استغلالاً فعليًا.
- ينفَّذ الكود ضمن سياق عملية IIS worker، ما قد يؤدي إلى اختراق كامل للخادم.
- المكتبة بلا مطوّر يصونها، وآخر إصدار لها Beta 0.9.1 يعود إلى ديسمبر 2008، ولا يتوفر تصحيح رسمي.
- أضافت CISA الثغرة إلى قائمة الثغرات المستغلة المعروفة وحددت ثلاثة أيام للجهات الفيدرالية

الأمريكية للمعالجة.

يستغل مهاجمون ثغرة غير مصححة في Idunno AntiCsrf، وهي وحدة مفتوحة المصدر للحماية من هجمات CSRF في تطبيقات ASP.NET WebForms. ولا يوجد مطوّر يصون هذه الوحدة، وآخر إصدار منها 0.9.1 Beta صدر في ديسمبر 2008.

ما الذي يحدث

الثغرة المسجلة برقم CVE-2026-131914 بدرجة CVSS تبلغ 9.3 هي خلل في إلغاء التسلسل غير الآمن. وبحسب WatchTowr، لا تتحقق المكتبة بالقدر الكافي من البيانات الواردة في نماذج الإدخال قبل إعادة بنائها ككائنات برمجية. وتفيد Mandiant بأن المهاجم يحتاج إلى طلب HTTP POST واحد فقط، دون مصادقة ودون رمز CSRF صالح، يتضمن قيمة غير فارغة في ملف تعريف الارتباط الخاص بـCSRF مع سلسلة gadget مشفرة بـBase64.

ولأن الفحص المعيب يعمل قبل منطق صفحات التطبيق نفسه، فقد يمس صفحات كثيرة في الموقع وليس صفحات تسجيل الدخول وحدها. وعند نجاح الهجوم يسيطر المهاجم على عملية IIS worker، ما قد يفضي إلى اختراق كامل للخادم. وقد رصدت Mandiant استغلالاً فعليًا، ورصدت WatchTowr محاولات فحص استغلالية على أنظمة الخداع (honeypots) لديها.

وأضافت CISA الثغرة إلى قائمة الثغرات المستغلة المعروفة، وطلبت من الجهات الفيدرالية الأمريكية معالجتها خلال ثلاثة أيام.

ما المطلوب

لا يوجد تصحيح رسمي، ويتوقع باحث WatchTowr ألا يصدر أي تصحيح. لذا ينبغي التوقف عن استخدام الوحدة والانتقال إلى بديل مدعوم. وإن تعذر الاستبدال فورًا، يمكن استخدام قواعد WAF كإجراء مؤقت إلى حين إيجاد حلول بديلة. وبالتوازي، ينبغي تحديد المنتجات المتأثرة ومراجعة سجلات التدقيق بحثًا عن مؤشرات استغلال.

ما يجب فعله الآن

1. حصر تطبيقات ASP.NET WebForms، بما فيها المنتجات الموردة من أطراف ثالثة، لتحديد ما يتضمن مكتبة Idunno.AntiCSRF.
2. استبدال المكتبة بحل مدعوم للحماية من CSRF، ومطالبة موردي المنتجات المتأثرة بجدول زمني للاستبدال.
3. تطبيق قواعد WAF أمام التطبيقات المتأثرة كإجراء مؤقت إذا تعذر الاستبدال الفوري.
4. مراجعة سجلات التدقيق للخوادم والتطبيقات بحثًا عن مؤشرات استغلال، والتعامل مع أي اشتباه باختراق خادم IIS بوصفه حادثًا.
5. تسجيل المسألة في سجلي الثغرات ومخاطر الأطراف الثالثة مع الإشارة إلى أنه لا يُتوقع صدور تصحيح.