CISA تحذّر من ثغرة إرسال بيانات غير مشفّرة في InterSystems IRIS for Health



نشرت CISA تنبيهاً طبياً بشأن InterSystems IRIS for Health، إذ يكون تشفير TLS/SSL معطّلًا افتراضياً، مما قد يتيح لمهاجم الاطلاع على البيانات المنقولة واستخدامها لتسجيل الدخول. درجة CVSS v3 هي 8.1.

- الثغرة CVE-2026-111594 تتعلق بنقل معلومات حساسة دون تشفير.
- تشفير TLS/SSL معطّل افتراضياً في InterSystems IRIS for Health.
- قد يطّلع المهاجم على البيانات المنقولة ويستخدمها لتسجيل الدخول إلى الجهاز.
- الإصدارات المذكورة: 2026.2.0.221 و2026.1.0.235 و2025.3.0.226.
- توصي الشركة بضبط IRIS superserver بحيث يشترط SSL/TLS.

أصدرت CISA تنبيهاً طبياً بشأن InterSystems IRIS for Health، وهو منتج يُستخدم في قطاع الرعاية الصحية والصحة العامة وينتشر عالمياً. ويقع المقر الرئيسي للشركة المطوّرة في الولايات المتحدة.

طبيعة المشكلة

يتناول التنبيه الثغرة CVE-2026-111594، وهي من فئة نقل المعلومات الحساسة دون تشفير. ففي IRIS for Health يكون تشفير TLS/SSL معطّلًا افتراضياً، وبالتالي قد يتمكن مهاجم قادر على مراقبة حركة البيانات من الاطلاع على البيانات المنقولة واستخدامها لتسجيل الدخول إلى الجهاز. ويمنح التنبيه الثغرة درجة 8.1 وفق CVSS v3.

الإصدارات المذكورة هي InterSystems IRIS for Health بالأرقام 2026.2.0.221 و2026.1.0.235 و2025.3.0.226.

المعالجة الموصى بها

توصي InterSystems المستخدمين بضبط IRIS superserver بحيث يشترط SSL/TLS، وتشرح وثائق الشركة المرتبطة بتنبيه CISA خطوات ذلك. ولا يذكر المصدر إصداراً مُصحّحاً ولا رصد استغلال للثغرة.

الدلالة للمؤسسات

لأن الضعف ناتج عن إعداد افتراضي، فقد تكون البيئات معرّضة حتى دون خلل برمجي بالمعنى المعتاد. لذا ينبغي لمقدمي الرعاية الصحية وكل جهة تشغّل IRIS for Health التحقق من إعدادات أنظمتها بدلًا من افتراض أن التشفير مفعّل.

ما يجب فعله الآن

1. حصر جميع نسخ InterSystems IRIS for Health وتوثيق إصداراتها.
2. التحقق من اشتراط SSL/TLS في IRIS superserver على كل نسخة.
3. ضبط superserver لاشتراط SSL/TLS وفق وثائق الشركة.
4. اختبار اتصالات العملاء والتكاملات بعد تفعيل التشفير لتفادي انقطاع الخدمة.
5. مراجعة سجلات الدخول وتدوير بيانات الاعتماد حيث يُحتمل تعرّضها دون تشفير على الشبكة.