ثغرة حقن شيفرة في Siemens ROS# قبل الإصدار 2.3.1 (CVE-2026-109097)



أصدرت CISA نشرة عن ثغرة حقن شيفرة في Siemens ROS# قبل الإصدار 2.3.1 (CVE-2026-109097، بدرجة CVSS 8.2). توصي Siemens بالتحديث إلى 2.3.1 أو أحدث.

- المتأثر: إصدارات Siemens ROS# الأقدم من 2.3.1.
- الثغرة CVE-2026-109097 مصنفة CWE-94 (حقن شيفرة) بدرجة CVSS تبلغ 8.2.
- لا يتم تهريب نص ملفات تعريف الرسائل بشكل سليم، فقد يتيح ملف مُعدّ خصيصاً حقن شيفرة عشوائية في البرنامج الناتج.
- الحل المعتمد من المورّد هو التحديث إلى الإصدار V2.3.1 أو أحدث.
- تدرج CISA قطاع التصنيع الحيوي، ومقر الشركة في ألمانيا.

ما الذي ورد في النشرة

نشرت CISA نشرة بشأن Siemens ROS# تفيد بأن الإصدارات السابقة للإصدار 2.3.1 تحتوي على ثغرة حقن شيفرة برمز CVE-2026-109097. صُنّفت الثغرة ضمن CWE-94 (ضعف التحكم في توليد الشيفرة)، وبلغت درجتها الأساسية وفق CVSS v3 ما مقداره 8.2.

آلية الثغرة

لا تقوم الإصدارات المتأثرة بتهريب نص ملفات تعريف الرسائل بالشكل الصحيح. فإذا تمكّن مهاجم من إيصال ملف تعريف رسائل مُعدّ خصيصاً إلى المستخدم، فقد يؤدي ذلك إلى حقن شيفرة عشوائية في البرنامج الذي تولّده الأداة. وتذكر النشرة قطاع التصنيع الحيوي، وأن المنتج منتشر حول العالم.

الاستجابة المقترحة

أصدرت Siemens نسخة مصححة وتوصي بالانتقال إلى V2.3.1 أو أحدث. ولا تذكر النشرة حلًا بديلًا مؤقتاً ولا بلاغات عن استغلال الثغرة، لذا فالتحديث هو المعالجة المعلنة.

ينبغي للمنشآت ذات البيئات الصناعية أو التصنيعية أن تحدد أولًا ما إذا كان ROS# مستخدماً لديها، ومنها فرق الهندسة والتطوير، وما الإصدارات المثبتة. وعند وجوده يُجدول التحديث عبر إدارة التغيير المعتادة، مع التعامل بحذر مع ملفات تعريف الرسائل الواردة من مصادر خارجية إلى حين التحديث.

ما يجب فعله الآن

1. حصر أي استخدام لـ Siemens ROS# لدى فرق الهندسة والتطوير والتقنية التشغيلية وتسجيل الإصدارات.
2. تحديث التثبيتات المتأثرة إلى V2.3.1 أو أحدث عبر إدارة التغيير.
3. تجنب استخدام ملفات تعريف الرسائل من مصادر غير موثوقة أو غير مُتحقق منها إلى حين التحديث.
4. مراجعة البرامج المولّدة من ملفات تعريف رسائل واردة من جهات خارجية بحثاً عن محتوى غير متوقع.
5. متابعة نشرات Siemens وCISA تحسباً لأي تحديثات.