سيمنز RUGGEDCOM CROSSBOW SAC: معالجة ثغرات SQLite في الإصدار 6.0



أعلنت CISA عن ثغرات متعددة في مكوّن SQLite ضمن RUGGEDCOM CROSSBOW Station Access Controller من سيمنز للإصدارات الأقدم من 6.0، بتقييم CVSS v3 قدره 9.8. وتوصي سيمنز بالتحديث إلى أحدث إصدار.

- المنتج المتأثر: RUGGEDCOM CROSSBOW Station Access Controller (SAC) بإصداراته الأقدم من 6.0.
- الثغرات في مكوّن SQLite المدمج وقد تتيح تنفيذ تعليمات برمجية أو حجب الخدمة أو الكشف عن معلومات حساسة.
- الثغرات المدرجة: CVE-2025-6965 وCVE-2025-70873 وCVE-2025-71316 وCVE-2026-11822 وCVE-2026-11824.
- تقييم CVSS v3 المذكور في النشرة هو 9.8.

- أصدرت سيمنز إصدارًا جديدًا وتوصي بالتحديث إلى أحدث إصدار.

ما الذي أُعلن

نشرت CISA نشرة استشارية خاصة بأنظمة التحكم الصناعي حول RUGGEDCOM CROSSBOW Station (SAC Access Controller) من سيمنز. يتضمن المنتج مكوّن SQLite يحتوي على عدة ثغرات، ووفق النشرة قد يستغلها مهاجم لتنفيذ تعليمات برمجية عشوائية أو التسبب في حجب الخدمة أو الحصول على معلومات حساسة.

تورد النشرة خمس ثغرات هي: CVE-2025-6965 وCVE-2025-70873 وCVE-2025-71316 وCVE-2026-11822 وCVE-2026-11824. ومن أنواع الضعف المذكورة: خطأ في اقتطاع القيم الرقمية، وعدم مسح ذاكرة الكومة قبل تحريرها، وسوء معالجة ترميز Unicode، وفيض في ذاكرة الكومة. ويبلغ تقييم CVSS v3 الخاص بالمورّد 9.8.

الجهات المتأثرة

تتأثر جميع إصدارات SAC الأقدم من 6.0. وتذكر CISA أن المنتج منتشر عالميًا، وتحدد القطاعات المعنية: التصنيع الحيوي، وأنظمة النقل، والطاقة، والرعاية الصحية والصحة العامة، والخدمات المالية، والخدمات والمرافق الحكومية. ويقع المقر الرئيس لسيمنز في ألمانيا.

الاستجابة المقترحة

أصدرت سيمنز إصدارًا جديدًا وتوصي بالانتقال إلى أحدث إصدار. ينبغي للمنشآت التحقق من وجود المنتج في بيئتها، ومراجعة الإصدار المثبّت، وجدولة التحديث عبر إجراءات إدارة التغيير المعتادة. ولا تشير النشرة إلى استغلال فعلي للثغرات، لذا يُبنى ترتيب الأولوية على درجة الخطورة ومدى تعرّض كل نظام.

ما يجب فعله الآن

1. مراجعة سجل الأصول للتحقق من وجود RUGGEDCOM CROSSBOW SAC وتوثيق الإصدار المثبّت.
2. جدولة التحديث إلى أحدث إصدار من سيمنز لأي نسخة أقدم من 6.0.
3. إلى حين التحديث، حصر الوصول الشبكي إلى أنظمة SAC على محطات الإدارة المصرّح بها فقط.
4. مراجعة سجلات SAC بحثًا عن توقفات غير متوقعة أو نشاط غير معتاد في قاعدة البيانات.
5. توثيق التعرض والمعالجة في سجل مخاطر التقنية التشغيلية ورفعها وفق الحوكمة الداخلية.