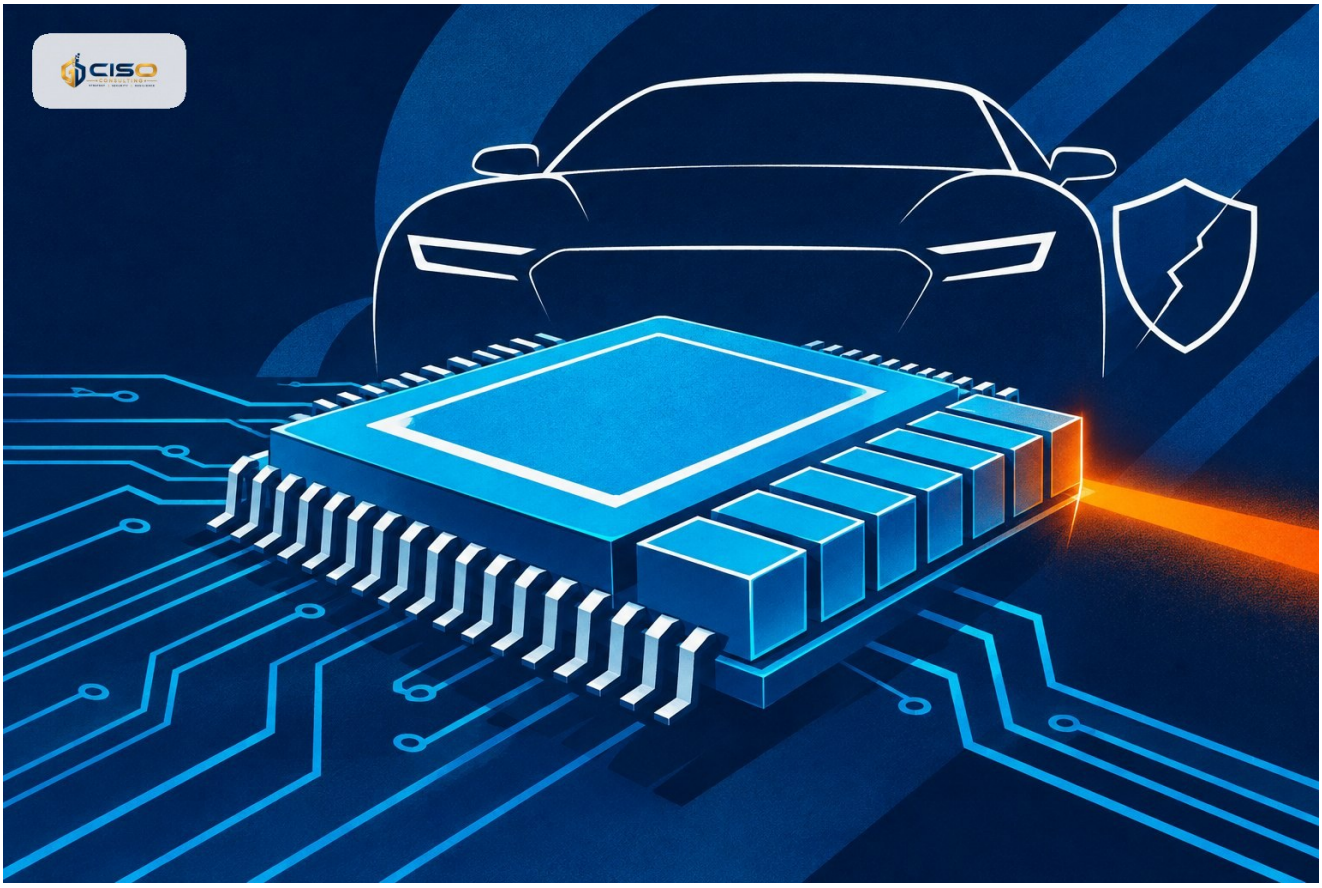
سيمنز Capital Embedded AR Classic: ثغرة قراءة خارج الحدود (CVE-2026-89208)



أصدرت CISA نشرة عن ثغرة قراءة خارج الحدود (CVSS v3: 5.3) CVE-2026-89208 في Capital Embedded AR Classic من سيمنز. أصدرت سيمنز نسخة مُصلحة من R20-11 وتُعدّ إصلاحات أخرى.

- الثغرة CVE-2026-89208 قراءة خارج الحدود سببها غياب التحقق من حدود المدخلات عند الوصول إلى بيانات الحزم.
- الإصدارات المتأثرة: Capital Embedded AR Classic 431-422 (كل الإصدارات) وR20-11 دون الإصدار 2303.
- قد يتسبب مهاجم عن بُعد دون مصادقة في سلوك غير طبيعي أو عدم استقرار أو حجب الخدمة.
- درجة CVSS v3 هي 5.3، وتوصي سيمنز بتحديث R20-11 إلى أحدث إصدار.
- حيثما لا يتوفر إصلاح بعد، توصي سيمنز بإجراءات تخفيف محددة.

ما الذي أُعلن

نشرت CISA نشرة عن ثغرة قراءة خارج الحدود، رقمها CVE-2026-89208، في Capital Embedded AR Classic من سيمنز. لا يتحقق المنتج بشكل سليم من حدود المدخلات قبل الوصول إلى بيانات الحزم، ما قد يتيح لمهاجم عن بُعد دون مصادقة التسبب في سلوك غير طبيعي أو عدم استقرار أو حجب الخدمة. وتبلغ درجة CVSS v3 في النشرة 5.3.

الإصدارات المتأثرة والإصلاحات

يشمل التأثير مجموعتين: Capital Embedded AR Classic 422-431 بكل إصداراته، وCapital Embedded AR Classic R20-11 في الإصدارات الأقل من 2303. أصدرت سيمنز نسخة جديدة لـ R20-11 وتوصي بالتحديث إلى أحدث إصدار، وتُعدّ إصلاحات إضافية، وتوصي بإجراءات تخفيف محددة للمنتجات التي لا يتوفر لها إصلاح بعد.

تذكر النشرة أن المنتج يُستخدم عالميًا في قطاعات منها التصنيع الحرج والنقل والطاقة والرعاية الصحية والخدمات المالية والمرافق الحكومية. ومقر سيمنز في ألمانيا.

ما المطلوب

التصنيف متوسط، لكن المنتج برمجية مضمّنة، وقد لا يظهر وجودها بوضوح في قوائم الأصول المعتادة. على الجهات التحقق أولاً مما إذا كانت أي أجهزة أو مكونات من الموردين لديها تتضمن هذه البرمجية، ثم اتباع إرشادات سيمنز للتحديث والتخفيف.

ما يجب فعله الآن

1. مراجعة سجل الأصول وسؤال الموردين عمّا إذا كانت الأجهزة تتضمن Capital Embedded AR Classic 422-431 أو R20-11.
2. تحديث نشرات R20-11 الأقل من الإصدار 2303 إلى أحدث إصدار من سيمنز بعد الاختبار.
3. تطبيق إجراءات التخفيف الواردة في نشرة سيمنز للإصدار 422-431 وأي منتجات لم يتوفر لها إصلاح.
4. متابعة إعلانات سيمنز بشأن نسخ الإصلاح الإضافية قيد الإعداد.
5. توثيق النتائج وحالة المعالجة في سجلات التقنية التشغيلية وإدارة الثغرات.