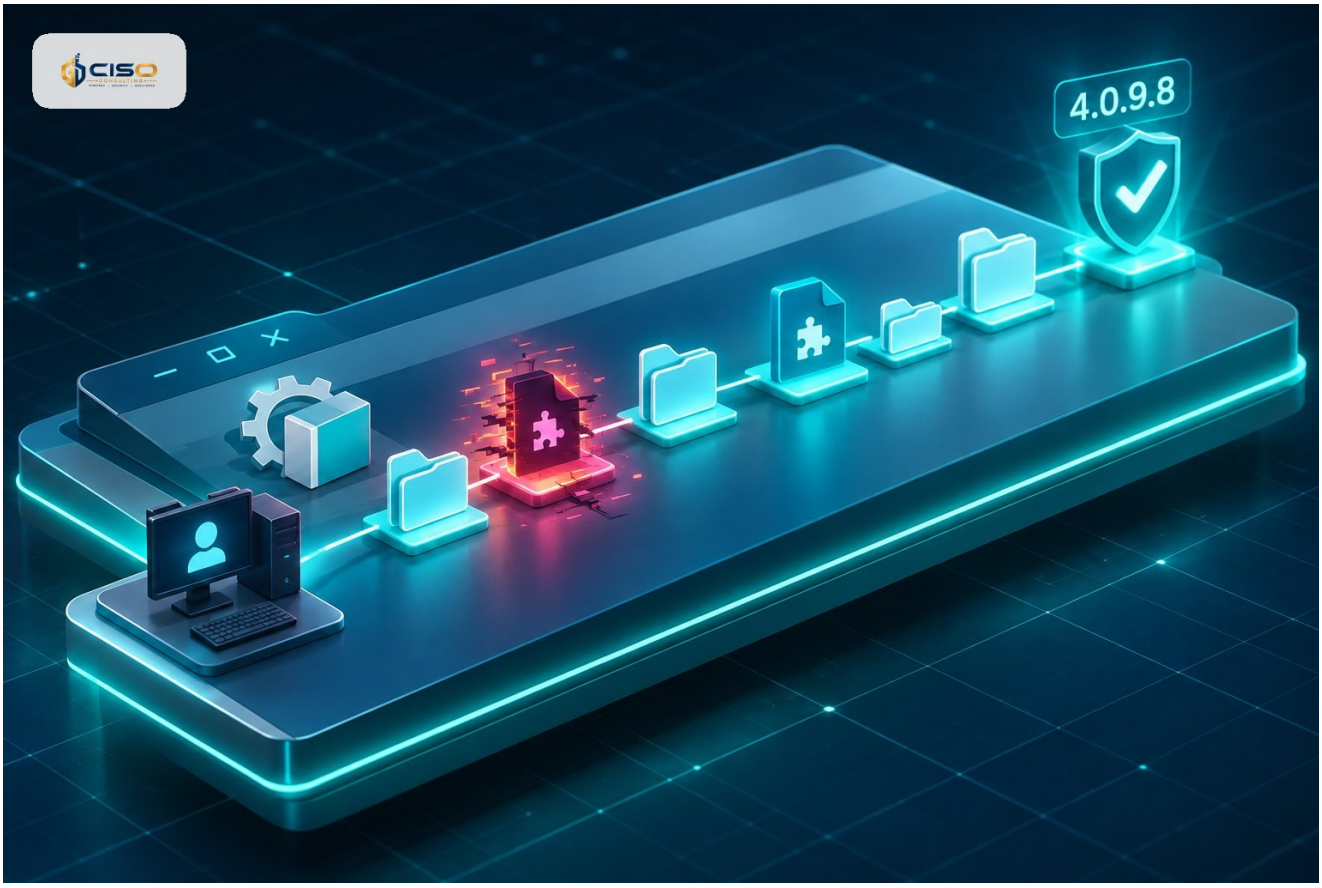
Siemens Software Center: معالجة ثغرة مسار البحث عن مكتبات DLL في الإصدار 4.0.9.8



أصدرت CISA تنبيهاً عن ثغرة في مسار البحث عن مكتبات DLL (CVE-2026-110936، CVSS v3: 6.7) في Siemens Software Center قبل 4.0.9.8، وتتيح لمهاجم محلي موثّق تنفيذ شيفرة. وتوصي Siemens بالتحديث.

- تؤثر الثغرة CVE-2026-110936 في إصدارات Siemens Software Center الأقدم من 4.0.9.8.
- يحمّل التطبيق مكتبات DLL من مسار بحث غير مضبوط.
- قد يتمكن مهاجم محلي موثّق من تنفيذ شيفرة عشوائية بصلاحيات التطبيق.
- درجة CVSS v3 هي 6.7، وقد أصدرت Siemens إصداراً مُعالجاً وتوصي بالتحديث.
- يشير التنبيه إلى مدونة تتناول الاستغلال الفعلي المعروف وطرق اكتشافه.

ما الذي ورد في التنبيه

نشرت CISA تنبيهاً يخص أنظمة التحكم الصناعي بشأن Siemens Software Center. يقوم التطبيق بتحميل مكتبات الربط الديناميكي (DLL) من مسار بحث غير مضبوط، وقد يتمكن مهاجم محلي موثّق من وضع مكتبة DLL مُعدّة خصيصاً في مجلد يبحث فيه التطبيق، فينفَّذ بذلك كود عشوائي بصلاحيات التطبيق.

تُتابَع الثغرة برقم **CVE-2026-110936** وبدرجة CVSS v3 تبلغ 6.7، وتشمل جميع الإصدارات الأقدم من 4.0.9.8. وقد أصدرت Siemens إصداراً جديداً وتوصي بالتحديث إلى أحدث إصدار.

أهمية الأمر

يذكر التنبيه أن المنتج منتشر عالمياً، وتشمل القطاعات المذكورة التصنيع الحيوي والطاقة والرعاية الصحية والخدمات المالية والخدمات الحكومية والنقل. كما يحيل إلى مدونة تتناول الاستغلال الفعلي المعروف حالياً وطرق اكتشافه، لذا ينبغي التعامل معه بما يتجاوز التحديث الروتيني.

يتطلب الاستغلال وصولًا محلياً ومصادقة، ما يحدّ من التعرض عن بُعد، لكن الكود المنفَّذ يعمل بصلاحيات التطبيق.

النهج المقترح

حدّدوا الأجهزة المثبَّت عليها Siemens Software Center وتحققوا من الإصدار، ثم جدولوا التحديث إلى 4.0.9.8 أو أحدث. راجعوا مرجع CISA الخاص بالكشف، وافحصوا الأجهزة المعنية بحثاً عن مكتبات DLL غير متوقعة في المجلدات التي يبحث فيها التطبيق.

ما يجب فعله الآن

1. حصر جميع عمليات تثبيت Siemens Software Center وتوثيق إصداراتها.
2. تحديث الأنظمة المتأثرة إلى الإصدار 4.0.9.8 أو أحدث وفق إجراءات إدارة التغيير.
3. مراجعة إرشادات الكشف المشار إليها في تنبيه CISA وفحص وجود مكتبات DLL غير متوقعة في مجلدات بحث التطبيق.
4. حصر الوصول المحلي وصلاحيات الكتابة على الأجهزة التي تشغّل البرنامج بالمستخدمين المصرّح لهم.
5. تسجيل الثغرة وإجراءات المعالجة في سجل إدارة الثغرات لأغراض الامتثال لضوابط NCA ECC وOTCC عند انطباقها.