Siemens Simcenter Femap: ثغرة قراءة خارج الحدود عند معالجة ملفات X_T (CVE-2026-64629)



أفادت CISA بوجود ثغرة قراءة خارج الحدود CVE-2026-64629 في إصدارات Simcenter Femap من Siemens الأقدم من V2606.0002، وقد يؤدي ملف X_T معدّ خصيصًا إلى تعطل التطبيق أو تنفيذ تعليمات برمجية. توصي Siemens بالتحديث.

- المتأثر: إصدارات Simcenter Femap الأقدم من V2606.0002.
- الثغرة CVE-2026-64629 من نوع قراءة خارج الحدود (CWE-125) تُستغل عند تحليل ملفات X_T.
- درجة CVSS v3.1 الأساسية 7.8 (عالية).
- الأثر: تعطل التطبيق أو تنفيذ تعليمات برمجية ضمن سياق العملية الحالية.
- المعالجة: التحديث إلى V2606.0002 أو أحدث.

ما الذي أُعلن

نشرت CISA نشرة بشأن تطبيق Simcenter Femap من Siemens، وهو تطبيق هندسي يرتبط بقطاع التصنيع الحيوي. يحتوي المنتج على ثغرة قراءة خارج الحدود برقم **CVE-2026-64629** تظهر عند تحليل الملفات بصيغة X_T.

قد يؤدي ملف X_T معدّ خصيصًا إلى تعطل التطبيق، أو يتيح للمهاجم تنفيذ تعليمات برمجية ضمن سياق العملية الحالية. صُنّفت الثغرة بدرجة 7.8 (عالية) وفق CVSS v3.1 ضمن CWE-125.

المتأثرون

تُدرج النشرة جميع إصدارات Simcenter Femap الأقدم من V2606.0002 ضمن الإصدارات المتأثرة. مقر Siemens في ألمانيا، وتشير النشرة إلى انتشار المنتج عالميًا. ولا يذكر المصدر وجود استغلال فعلي للثغرة.

الاستجابة الموصى بها

أصدرت Siemens نسخة مصححة وتوصي بالتحديث إلى V2606.0002 أو أحدث. ينبغي للجهات التي تستخدم Femap، خصوصًا في البيئات الهندسية والصناعية والتصنيعية، حصر الإصدارات المثبتة وجدولة التحديث عبر إجراءات إدارة التغيير المعتادة. ولأن الاستغلال يبدأ بملف، فمن الحكمة التعامل بحذر مع ملفات X_T الواردة من مصادر غير موثوقة إلى حين اكتمال التحديث.

ما يجب فعله الآن

1. حصر جميع تثبيتات Simcenter Femap وتوثيق إصداراتها.
2. تحديث التثبيتات المتأثرة إلى V2606.0002 أو أحدث عبر إدارة التغيير.
3. التعامل بحذر مع ملفات X_T الواردة من مصادر غير موثوقة أو خارجية إلى حين التحديث.
4. تقييد من يستطيع تشغيل Femap وفتح الملفات الخارجية على محطات العمل الهندسية.
5. توثيق المعالجة في سجل إدارة الثغرات.