

سيمنس تعالج ثغرة DLL sideloading في Siemens Software Center استُغلت في هجمات ClickFix



عالجت سيمنس الثغرة CVE-2026-110936 عالية الخطورة في Siemens Software Center، وهي من نوع DLL sideloading، وأفادت باستغلالها في هجمات ClickFix. يُنصح بتطبيق التحديث.

- عالجت سيمنس ثغرة DLL sideloading في Siemens Software Center.
- تحمل الثغرة الرمز CVE-2026-110936 بدرجة CVSS v4 تبلغ 8.4 (عالية).
- يمكن للمهاجم الذي يضع ملف DLL مُعدّاً في مجلد يبحث فيه التطبيق تنفيذ شيفرة خبيثة.
- تُنفَّذ الشيفرة بالصلاحيات نفسها التي يعمل بها التطبيق.
- أفادت سيمنس باستغلال الثغرة في هجمات ClickFix.

ما الذي أُعلن

أصدرت سيمنس تحديثاً يعالج ثغرة من نوع DLL sideloading في Siemens Software Center، وذكرت أن الثغرة استُغلت في هجمات ClickFix. وتحمل الثغرة الرمز CVE-2026-110936 ودرجة CVSS v4 تبلغ 8.4، أي ضمن فئة الخطورة العالية.

كيف تعمل الثغرة

يحدث DLL sideloading عندما يحلّ التطبيق مكتبة من موقع يستطيع المهاجم التأثير فيه. وفي هذه الحالة يمكن للمهاجم وضع ملف DLL مُعدّ خصيصاً في مجلد يبحث فيه التطبيق، فينفذ التطبيق شيفرة المهاجم بالصلاحيات نفسها التي يعمل بها.

ويربط المصدر الاستغلال بهجمات ClickFix، وهي هجمات تعتمد عادةً على إقناع المستخدم بتنفيذ إجراء بنفسه. ولا يتضمن المقتطف تفاصيل إضافية عن الحملات أو الإصدارات المتأثرة أو الإصدار المُصحَّح، لذا ينبغي التأكد منها من نشرة سيمنس الأمنية.

أهمية الأمر للجهات المنظّمة

غالباً ما تُثبت أدوات الموردين الهندسية والصناعية على محطات عمل بصلاحيات مرتفعة. ولذلك قد يكون أثر ثغرة تنفذ شيفرة بصلاحيات التطبيق أكبر مما توجي به تسميتها. وعلى الجهات التحقق من وجود Siemens Software Center في بيئتها والتعامل مع التحديث كأولوية.

ما يجب فعله الآن

1. حصر جميع الأنظمة المثبت عليها Siemens Software Center.
2. مراجعة نشرة سيمنس الخاصة بالثغرة CVE-2026-110936 وتطبيق التحديث دون تأخير.
3. فحص مجلدات التطبيق على تلك الأنظمة بحثاً عن ملفات DLL غير متوقعة.
4. حصر صلاحية الكتابة في مجلدات التطبيق ومسارات البحث على مسؤولي النظام.
5. تذكير الموظفين بعدم لصق أو تشغيل أوامر من صفحات ويب أو رسائل، فهجمات ClickFix تعتمد على ذلك.