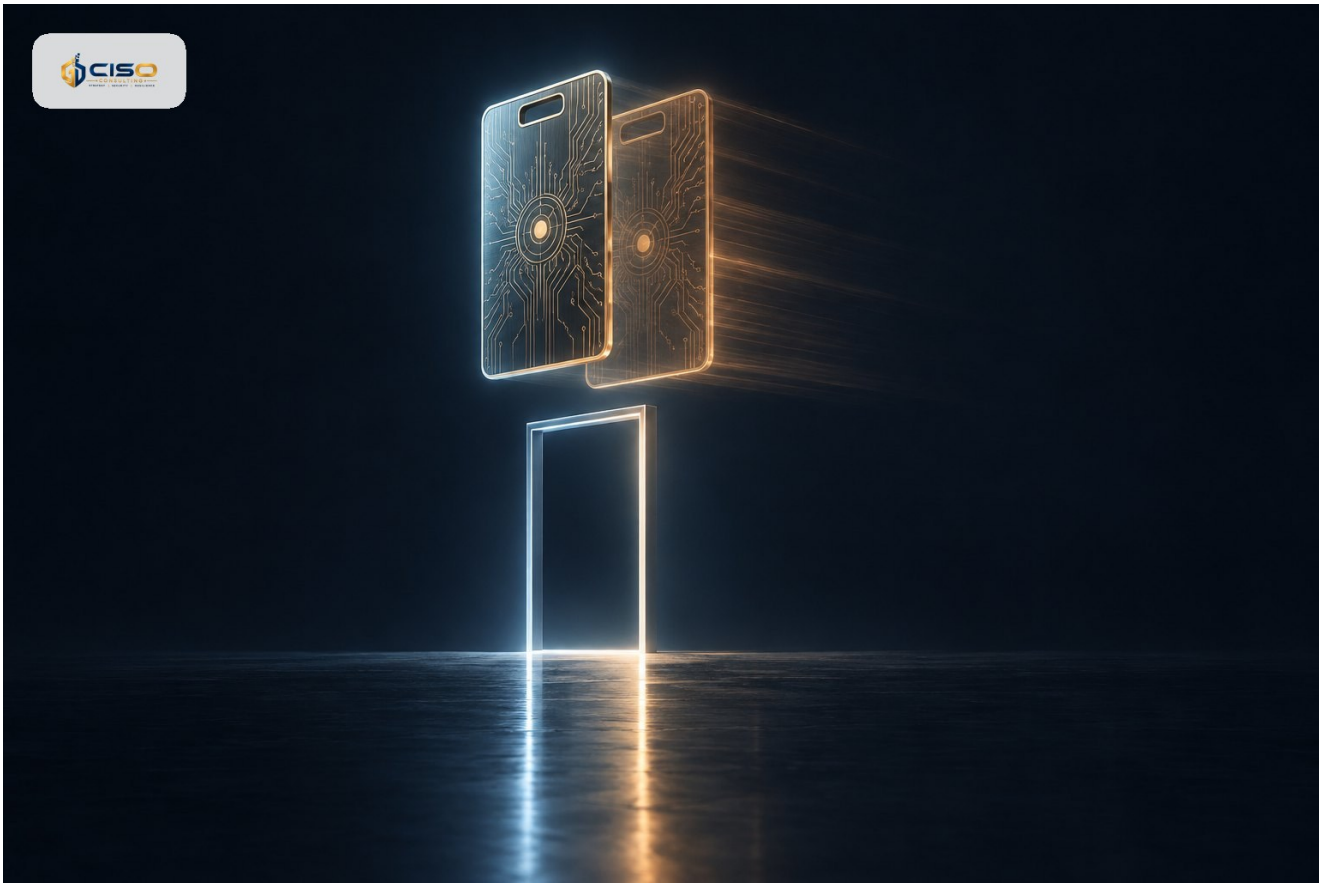
وحدة Mendix SAML من Siemens: تجاوز المصادقة عبر إعادة استخدام تأكيدات SAML (CVE-2026-89209)



أفادت CISA بوجود ثغرة إعادة استخدام في وحدة Mendix SAML من Siemens قد تتيح لمهاجم عن بُعد دون مصادقة الوصول عبر تسجيل الدخول الذي يبدأه مزوّد الهوية. وقد أصدرت Siemens إصدارات مصححة.

- الثغرة CVE-2026-89209 تجاوز للمصادقة ناتج عن ضعف الحماية من إعادة استخدام تأكيدات SAML.
- تمس مسارات المصادقة التي يبدأها مزوّد الهوية، ويمكن استغلالها عن بُعد دون مصادقة.
- الإصدارات المتأثرة: وحدات Mendix 10 و11 دون 4.2.4، ووحدات Mendix 9 دون 3.6.29.
- درجة CVSS v3 تبلغ 6.8.
- توصي Siemens بالتحديث إلى أحدث الإصدارات.

نشرت CISA تنبيهًا بشأن ثغرة تجاوز مصادقة في وحدة Mendix SAML من Siemens، تحمل الرمز CVE-2026-89209. فالوحدة لا تحمي بالقدر الكافي من إعادة استخدام تأكيدات SAML في المسارات التي يبدؤها مزوّد الهوية (IdP).

ما الذي يتأثر

قد يتمكن مهاجم عن بُعد دون مصادقة من إعادة استخدام تأكيد SAML صالح للحصول على وصول غير مصرح به إلى التطبيق. والإصدارات المتأثرة هي:

- Mendix SAML (متوافق مع Mendix 10): الإصدارات الأقدم من 4.2.4
- Mendix SAML (متوافق مع Mendix 11): الإصدارات الأقدم من 4.2.4
- Mendix SAML (متوافق مع Mendix 9): الإصدارات الأقدم من 3.6.29

ويذكر التنبيه درجة CVSS v3 قدرها 6.8، ويحدد قطاعي التصنيع الحرج وتقنية المعلومات، مع انتشار عالمي. ويقع المقر الرئيسي لشركة Siemens في ألمانيا.

الخطوات المقترحة

أصدرت Siemens إصدارات جديدة وتوصي بالتحديث إلى أحدثها. وينبغي للجهات التي تبني تطبيقاتها على Mendix وتستخدم وحدة SAML للدخول الموحد أن تحدد أولاً التطبيقات التي تتضمنها وإصدار كل منها، ثم تجدول التحديث بحسب انكشاف كل تطبيق، بادئةً بالتطبيقات المتاحة عبر الإنترنت.

لا يشير المصدر إلى استغلال فعلي للثغرة، لذا فهي مهمة ترقيع ذات أولوية وليست حالة طارئة. ومع ذلك يحسن اختبار التحديث في بيئة تجريبية قبل الإصدار، ومراجعة سجلات المصادقة بحثًا عن عمليات دخول متكررة غير معتادة.

ما يجب فعله الآن

1. حصر تطبيقات Mendix التي تستخدم وحدة SAML وتسجيل إصدار الوحدة في كل منها.
2. التحديث إلى أحدث الإصدارات الصادرة عن Siemens، بدءًا بالتطبيقات المتاحة عبر الإنترنت.
3. اختبار التحديث في بيئة غير إنتاجية قبل الإصدار.
4. مراجعة سجلات المصادقة بحثًا عن عمليات دخول متكررة أو غير معتادة عبر مزوّد الهوية.
5. توثيق الثغرة وإجراءات المعالجة في سجل إدارة الثغرات.