Siemens SIMATIC WinCC: ثغرة رفع صلاحيات في قاعدة البيانات (CVE-2026-59241)



أعلنت CISA عن ثغرة صلاحيات في قاعدة بيانات SIMATIC WinCC بالإصدارات V7.5 وV8.0 وV8.1 (CVE-2026-59241)، بدرجة CVSS 8.8). وتوصي Siemens بالتحديث وتطبيق إجراءات التخفيف حيث لا يتوفر إصلاح.

- الثغرة CVE-2026-59241 تتعلق بمنح صلاحيات غير صحيحة، وتبلغ درجتها 8.8 وفق CVSS v3.
- يمكن لمستخدم موثّق لديه وصول إلى قاعدة البيانات تنفيذ أوامر على النظام المضيف.
- الإصدارات المتأثرة: WinCC V7.5 (جميع الإصدارات)، وV8.0 قبل 8.0.0.11، وV8.1 قبل 8.1.7.
- أصدرت Siemens إصدارات جديدة لعدة منتجات وتعمل على إصلاحات إضافية.
- يوصى بإجراءات تخفيف للمنتجات التي لم يتوفر لها إصلاح بعد.

ما الذي أُعلن

نشرت CISA نشرة بشأن ثغرة في عدة إصدارات من Siemens SIMATIC WinCC. فالتطبيق لا يقيّد بما يكفي الصلاحيات الممنوحة لدور في قاعدة البيانات، ما قد يتيح لمستخدم موثّق لديه وصول إلى القاعدة تنفيذ أوامر على النظام المضيف. تحمل الثغرة المعرّف **CVE-2026-59241** ودرجة 8.8 وفق CVSS v3.

الإصدارات المتأثرة واستجابة المورّد

تشمل النشرة SIMATIC WinCC V7.5 (جميع الإصدارات)، وإصدارات V8.0 الأقدم من 8.0.0.11، وإصدارات V8.1 الأقدم من 8.1.7. أصدرت Siemens نسخًا جديدة لعدد من المنتجات المتأثرة وتوصي بالانتقال إلى أحدث الإصدارات. وتعمل على إصلاحات إضافية، وتوصي بإجراءات تخفيف للمنتجات التي لا يتوفر لها إصلاح حاليًا.

وتشير CISA إلى أن المنتج منتشر عالميًا ويُستخدم في قطاعات منها التصنيع الحرج والطاقة والنقل والرعاية الصحية والخدمات المالية والمرافق الحكومية.

الخطوات التالية

لأن الاستغلال يتطلب حسابًا موثّقًا لديه وصول إلى قاعدة البيانات، فالأولوية هي معرفة أماكن تشغيل WinCC ومن يستطيع الوصول إلى قاعدته. خطّطوا للتحديث إلى الإصدارات المصححة، وطبّقوا لإصدار V7.5 إجراءات التخفيف الواردة في نشرة Siemens إلى حين توفر إصلاح. وأخضعوا أي تغيير على أنظمة التحكم الإنتاجية لإجراءات إدارة التغيير والاختبار المعتادة.

ما يجب فعله الآن

1. حصر جميع تثبيتات SIMATIC WinCC وتسجيل إصداراتها ومطابقتها بالنطاقات المتأثرة.
2. مراجعة الحسابات التي لديها وصول إلى قاعدة بيانات WinCC وإزالة غير الضروري منها.
3. جدولة التحديث إلى V8.0.0.11 أو أحدث وV8.1.7 أو أحدث مع الاختبار قبل التطبيق في بيئة الإنتاج.
4. تطبيق إجراءات التخفيف الواردة في نشرة Siemens لإصدار V7.5 وأي منتج لا يتوفر له إصلاح.
5. حصر الوصول الشبكي إلى خدمات قاعدة بيانات WinCC على الأجهزة المصرّح بها ومراقبة أي تنفيذ أوامر غير معتاد.