CISA تحذّر من ثغرتين في PowerSYSTEM Center من Subnet Solutions



نشرت CISA إشعارًا عن ثغرتين في PowerSYSTEM Center المستخدم في قطاعي الطاقة والتصنيع الحيوي، تتيحان تنفيذ أوامر SQL غير مصرّح بها والوصول إلى موارد مقيّدة في إصدارات 2020 و2024 و2026.

- CVE-2026-63017 ثغرة تفويض غير سليم تتيح لمستخدم موثّق محدود الصلاحيات الوصول إلى موارد مخصصة للمسؤولين.
- CVE-2026-63774 مدرجة مع حقن SQL كنوع ثانٍ من الضعف، وتخص إصدارات 2024 و2026.
- الإصدارات المتأثرة: 2020 حتى x.5.29، و2024 من x.6.0 إلى x.6.2، و2026 من x.7.0 إلى x.7.1.
- يذكر الإشعار تقييم CVSS v3 بدرجة 9 ويحدد قطاعي الطاقة والتصنيع الحيوي.
- المقر الرئيسي للشركة المصنّعة في كندا والمنتج منتشر عالميًا.

أصدرت CISA إشعارًا خاصًا بأنظمة التحكم الصناعي يتعلق بمنتج PowerSYSTEM Center من Subnet Solutions. ويصف الإشعار ثغرتين قد تتيحان للمهاجم، عند استغلالهما، تنفيذ أوامر SQL غير مصرّح بها والوصول إلى موارد لا يحق له الوصول إليها.

ما الذي تأثر

يذكر الإشعار ثلاثة خطوط إصدار: PowerSYSTEM Center 2020 حتى x.5.29، وPowerSYSTEM Center 2024 من x.6.0 إلى x.6.2، وPowerSYSTEM Center 2026 من x.7.0 إلى x.7.1. وتنطبق CVE-2026-63017 على الإصدارات الثلاثة، بينما تنطبق CVE-2026-63774 على إصداري 2024 و2026.

تتعلق CVE-2026-63017 بتفويض غير سليم، إذ يستطيع مستخدم موثّق ذو صلاحيات محدودة الوصول إلى موارد مقتصرة عادةً على المسؤولين. كما يدرج الإشعار حقن SQL ضمن أنواع الضعف. ويعرض تقييم CVSS v3 بدرجة 9، ويحدد قطاعي التصنيع الحيوي والطاقة.

الخطوات المقترحة

يشير مقتطف المصدر إلى توصيات تخفيف من الشركة لمستخدمي PowerSYSTEM Center 2024 دون إيراد نصها كاملاً. لذا ينبغي الاطلاع على إشعار CISA الكامل وتعليمات الشركة قبل تخطيط أي تغيير.

وعلى الجهات العاملة في الطاقة والعمليات الصناعية أن تحدد أولاً هل المنتج موجود في بيئتها، وأي إصدار يعمل، ومن يملك حسابات عليه. ولأن إحدى الثغرتين تتطلب حسابًا موثّقًا، فإن مراجعة صلاحيات الحسابات خطوة مناسبة مبكرة ريثما تُجدول المعالجة.

ما يجب فعله الآن

1. حصر أي تركيبات لـ PowerSYSTEM Center إصدار 2020 أو 2024 أو 2026 وتسجيل الإصدارات بدقة.
2. قراءة إشعار CISA الكامل وتوصيات الشركة للتخفيف، وتخطيط المعالجة وفقًا لها.
3. مراجعة الحسابات على المنصة وإزالة الوصول الزائد أو غير الضروري للمستخدمين محدودي الصلاحيات.
4. التأكد من أن المنصة غير متاحة من شبكات غير موثوقة وأن الوصول مقصور على المستخدمين المطلوبين.
5. مراقبة سجلات قاعدة البيانات والتطبيق بحثًا عن استعلامات غير معتادة أو نشاط بمستوى مسؤول من حسابات عادية.