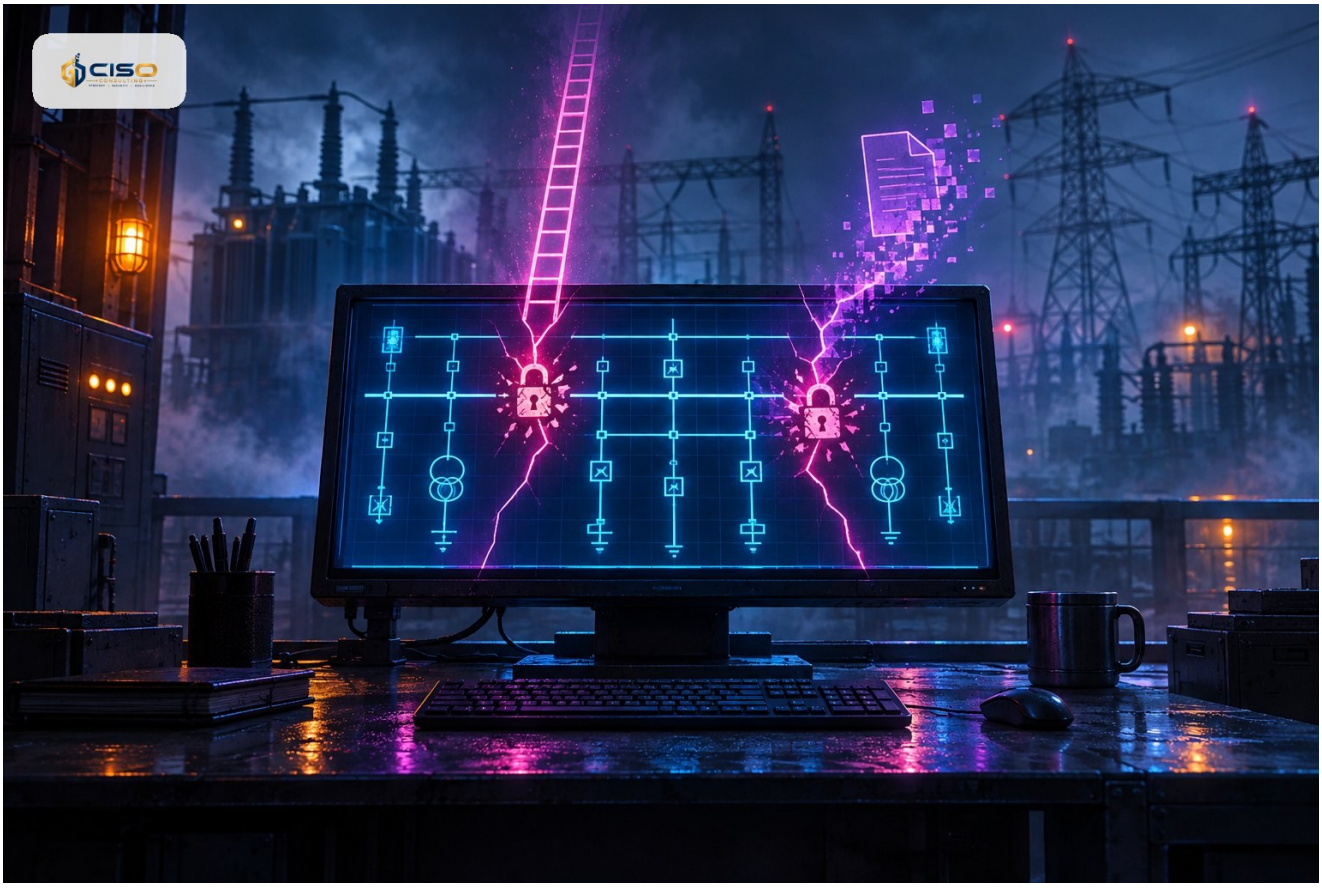
CISA تنبّه إلى ثغرتين في ABB PCM600 حتى الإصدار 2.14



نشرت CISA تنبيهاً بشأن ABB PCM600 حتى الإصدار 2.14، يتضمن ثغرتين (CVE-2026-15952 وCVE-2026-15953) قد تتيحان رفع الصلاحيات أو الكتابة فوق ملفات، بتقييم CVSS v3 بلغ 6.4.

- المنتج المتأثر: ABB Protection and Control IED Manager PCM600 بإصداراته حتى 2.14 ضمناً.
- الثغرة CVE-2026-15952 تخص خدمة Scheduler التي تعمل بحساب LocalSystem بينما يملك مستخدمو PCM600 العاديون صلاحيات عليها.
- الاستغلال يتطلب وصولًا محلياً وبيانات دخول صالحة، وقد ينتهي بالسيطرة على الجهاز.
- الثغرة الثانية CVE-2026-15953 من نوع اجتياز المسار، ومن الآثار المحتملة المذكورة الكتابة فوق ملفات.
- يذكر التنبيه قطاع الطاقة والانتشار عالمياً ودرجة CVSS v3 تساوي 6.4.

ما الذي نُشر

أصدرت CISA تنبيهاً خاصاً بأنظمة التحكم الصناعي بشأن ABB Protection and Control IED Manager PCM600 في إصداراته حتى 2.14 ضمناً. يتضمن التنبيه ثغرتين هما CVE-2026-15952 وCVE-2026-15953، ويذكر أن استغلالهما قد يتيح للمهاجم رفع صلاحياته أو الكتابة فوق ملفات. بلغت درجة CVSS v3 6.4. وتقع المقر الرئيسي لشركة ABB في سويسرا، ويصنّف التنبيه المنتج ضمن قطاع الطاقة مع انتشار عالمي.

التفاصيل التقنية

تتعلق CVE-2026-15952 بخدمة Scheduler المثبّتة مع PCM600. تعمل هذه الخدمة بحساب LocalSystem، في حين تُمنح الصلاحيات عليها لمستخدمي PCM600 العاديين عبر عضويتهم في مجموعة المستخدمين المحليين. ويمكن لمهاجم يملك وصولًا محلياً وبيانات دخول صالحة استغلال ذلك لرفع الصلاحيات والسيطرة على الجهاز المتأثر. أما الثغرة CVE-2026-15953 فمصنفة كضعف في اجتياز المسار (تقييد غير سليم لمسار الملف ضمن مجلد محدد)، ولا يتناول المقتطف المتاح تفاصيل إضافية عنها.

القراءة العملية

تفترض الثغرتان أن المهاجم يملك موطئ قدم على الجهاز أصلًا، لذا يتركز التعرض في من يستطيع تسجيل الدخول إلى محطات الهندسة التي تشغّل PCM600. وعلى الجهات العاملة في الطاقة والمرافق التأكد من استخدام PCM600 ومن الإصدار المثبّت. ولا يوضح المقتطف توفر إصدار مصحَّح، لذا يُرجع إلى تنبيه CISA الكامل وإشعار ABB للاطلاع على إرشادات المعالجة.

ما يجب فعله الآن

1. حصر جميع الأجهزة التي تشغّل PCM600 وتسجيل الإصدار المثبّت ومقارنته بالحد 2.14.
2. مراجعة تنبيه CISA الكامل وإشعار ABB للاطلاع على الإصلاحات أو إجراءات التخفيف والتخطيط لتطبيقها.
3. حصر الدخول التفاعلي والبعيد إلى محطات PCM600 في المهندسين المحددين الذين يحتاجونه فعلًا.
4. مراجعة عضوية مجموعة المستخدمين المحليين على هذه الأجهزة وإزالة الحسابات التي لا تحتاج إلى وصول.
5. مراقبة هذه المحطات لرصد أي تغيّر غير متوقع في الصلاحيات أو تعديل في الملفات وفق ضوابط أمن التقنيات التشغيلية.