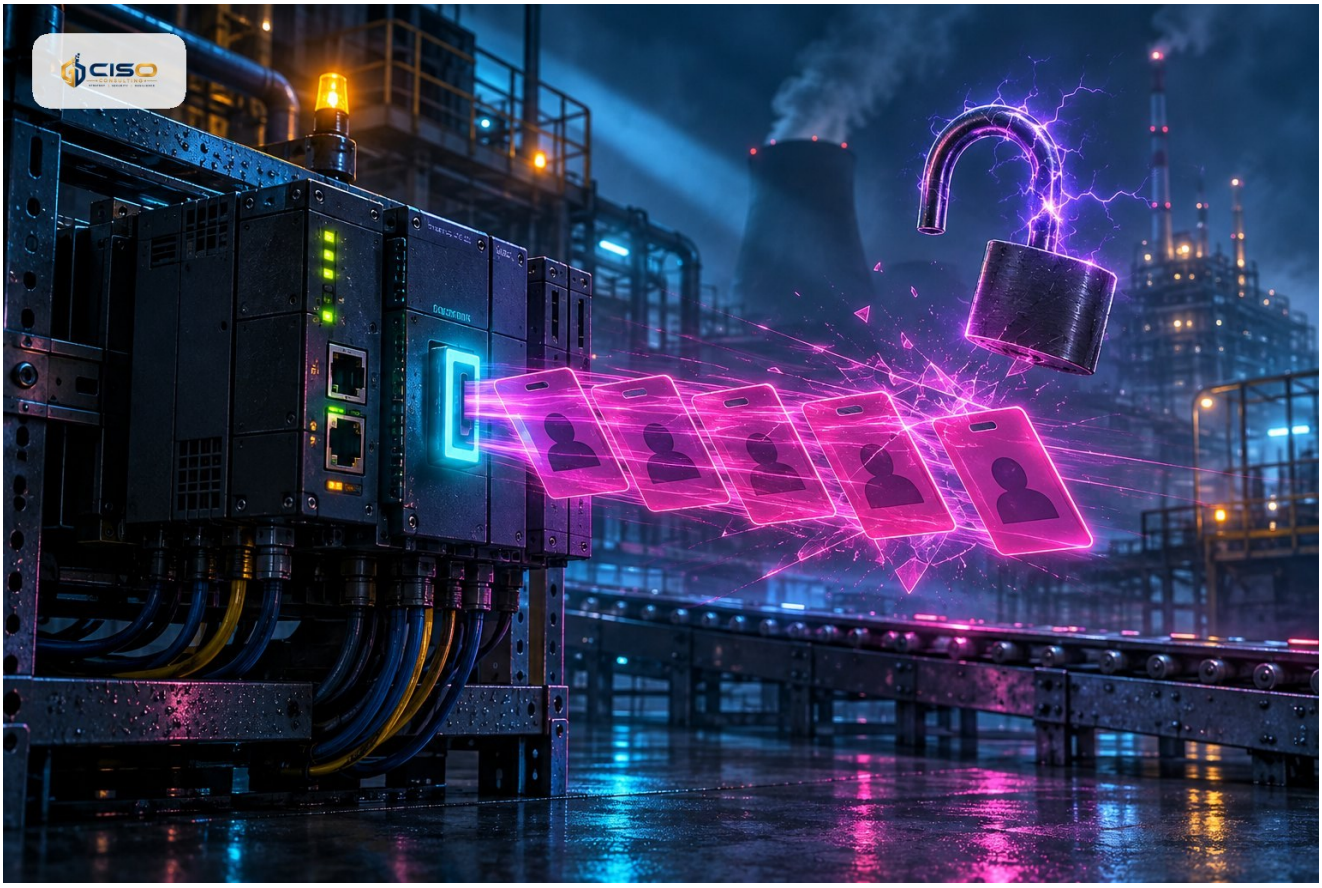
CISA تحذّر من ثغرة تزامن في OpenPLC Runtime تتيح إنشاء حسابات مسؤول دون مصادقة



أصدرت CISA تنبيهاً عن الثغرة CVE-2026-126088 في OpenPLC Runtime بالإصدار 4.2.4 وما قبله، إذ قد يؤدي تزامن الطلبات إلى إنشاء عدة حسابات مسؤول دون مصادقة. والمعالجة بالتحديث إلى 4.3.0 أو أحدث.

- المنتج المتأثر: Autonomy Logic OpenPLC Runtime بالإصدار 4.2.4 وما قبله.
- الثغرة CVE-2026-126088 من نوع حالة تسابق (CWE-362) بتقييم CVSS v3 يبلغ 8.1.
- تمرّ الطلبات المتزامنة فحص الوجود قبل حفظ أي مستخدم، فتُنشأ عدة حسابات مسؤول دون مصادقة.
- المعالجة من المورّد: التحديث إلى OpenPLC Runtime 4.3.0 أو أحدث.
- القطاعات المذكورة: التصنيع الحيوي والطاقة وأنظمة النقل والمياه والصرف الصحي.

نشرت CISA تنبيهاً خاصاً بأنظمة التحكم الصناعي بشأن OpenPLC Runtime من Autonomy Logic، ويتناول ثغرة واحدة هي CVE-2026-126088 تمس الإصدار 4.2.4 وما قبله.

طبيعة المشكلة

الثغرة من نوع حالة تسابق (CWE-362). فعند وصول عدة طلبات في اللحظة نفسها، قد تجتاز جميعها فحص وجود المستخدم قبل حفظ أي حساب. ووفق التنبيه، تكون النتيجة إنشاء عدة حسابات مسؤول دون مصادقة. وتبلغ درجة CVSS v3 للثغرة 8.1.

يذكر التنبيه قطاعات التصنيع الحيوي والطاقة وأنظمة النقل والمياه والصرف الصحي، مع انتشار المنتج عالمياً، ومقر الشركة في الولايات المتحدة.

الإجراء المطلوب

معالجة المورّد هي التحديث إلى OpenPLC Runtime 4.3.0 أو أحدث. وعلى الجهات التي تشغّل هذا المنتج في بيئات التقنية التشغيلية أن تحدد أولًا ما إذا كانت لديها نسخة بالإصدار 4.2.4 أو أقدم، ثم تخطط للتحديث عبر إجراءات إدارة التغيير المعتمدة لبيئة OT. ولا يذكر المصدر استغلالًا فعلياً للثغرة ولا حلولًا بديلة، لذا لا نفترض شيئاً في ذلك.

ولأن الأثر هو وصول إداري غير مصرّح به، فمن المناسب أيضاً مراجعة الحسابات الموجودة على النسخ المتأثرة والتحقق من خلوها من حسابات غير متوقعة.

ما يجب فعله الآن

1. حصر جميع نسخ OpenPLC Runtime وتحديد ما كان منها بالإصدار 4.2.4 أو أقدم.
2. تحديث النسخ المتأثرة إلى OpenPLC Runtime 4.3.0 أو أحدث عبر إجراءات إدارة التغيير في بيئة OT.
3. مراجعة حسابات المستخدمين على النسخ المتأثرة والتحقيق في أي حسابات مسؤول غير متوقعة.
4. التأكد من عدم إمكانية الوصول إلى واجهات إدارة OpenPLC من شبكات غير موثوقة.
5. تسجيل الثغرة وحالة المعالجة في سجل مخاطر التقنية التشغيلية.