

ثغرات حقن CSV وخلل في خوارزمية المصادقة: Hitachi Energy MicroSCADA X SYS600: الكشف عن



نشرت CISA تنبيهاً عن ثغرات في Hitachi Energy MicroSCADA X SYS600 من الإصدارات حتى 10.7 والإصدار 10.8، تشمل حقن معادلات CSV وخللاً في خوارزمية المصادقة، بدرجة CVSS v3 تبلغ 7.8.

- الإصدارات المتأثرة: Hitachi Energy MicroSCADA X SYS600 حتى 10.7، والإصدار 10.8.
- الثغرات المذكورة: CVE-2026-9852 و CVE-2026-9853 و CVE-2026-9854.
- نوعا الضعف: عدم معالجة عناصر المعادلات في ملفات CSV بشكل سليم، وتنفيذ غير صحيح لخوارزمية المصادقة.
- درجة CVSS v3 لدى المورّد 7.8، والمنتج مستخدم في قطاع الطاقة.
- توفّر Hitachi Energy خطوات التخفيف والمعالجة ضمن قسم الإجراءات الفورية الموصى بها.

ما الذي أُعلن عنه

نشرت CISA تنبيهاً يخص أنظمة التحكم الصناعي ويتناول عدة ثغرات في Hitachi MicroSCADA X SYS600 من Hitachi Energy. تشمل الإصدارات المتأثرة كل ما هو حتى 10.7 بما فيه، إضافة إلى الإصدار 10.8. ويذكر التنبيه الثغرات CVE-2026-9852 و CVE-2026-9853 و CVE-2026-9854، وتبلغ درجة CVSS v3 التي حددها الموزّع 7.8.

يسمّي التنبيه فئتين من الضعف: عدم معالجة عناصر المعادلات في ملفات CSV بشكل سليم، وتنفيذ غير صحيح لخوارزمية المصادقة. والمنتج مرتبط بقطاع الطاقة ويُستخدم عالمياً، ومقر الشركة في سويسرا.

مشكلة حقن CSV

في CVE-2026-9852 يصف التنبيه ثغرة حقن CSV في SYS600. إذ يمكن لمعادلات خبيثة داخل البيانات المصدّرة أن تضيف محتوى إلى جدول البيانات أو تعدّله، أو تُدرج روابط، أو تسرّب بيانات، وقد تنفّذ شيفرة خبيثة على جهاز المستخدم بحسب إعدادات بيئته. ولا يعرض المقتطف المتاح شروط الاستغلال الكاملة ولا تفاصيل الثغرات الأخرى.

الخطوات التالية

يوجّه الموزّع عملاءه إلى قسم الإجراءات الفورية الموصى بها للتخفيف والمعالجة. وعلى مشغلي SYS600 التأكد مما إذا كانوا يستخدمون إصداراً متأثراً، ومراجعة التنبيه الكامل وإرشادات الموزّع، والتخطيط للمعالجة عبر إجراءات إدارة التغيير المعتمدة لبيئات التقنية التشغيلية.

ما يجب فعله الآن

1. حصر جميع نسخ SYS600 والتحقق مما إذا كانت بالإصدار 10.7 أو أقدم، أو 10.8.
2. قراءة تنبيه CISA كاملاً والإجراءات الفورية الموصى بها من Hitachi Energy، ثم جدولة التخفيف أو المعالجة.
3. إلى حين المعالجة، التعامل مع ملفات CSV المصدّرة من SYS600 كم ملفات غير موثوقة وتجنب فتحها مع تفعيل الماكرواوت أو المعادلات.
4. مراجعة صلاحيات الوصول إلى SYS600 وعزل الشبكة ضمن إدارة مخاطر التقنية التشغيلية.
5. تسجيل التعرض وخطة المعالجة في سجل مخاطر التقنية التشغيلية.