CISA تحذّر من ثغرات في منتج InfoScan من Dorsett Controls المستخدم في قطاع المياه



نشرت CISA تنبيهًا بشأن InfoScan من Dorsett Controls حتى الإصدار 1.45.0 يشمل ست ثغرات، وقد يتيح استغلالها كشف بيانات وبيانات اعتماد أو اعتراض الاتصالات والتلاعب بها.

- المتأثر: InfoScan من Dorsett Controls بالإصدار 1.45.0 وما قبله.
- ست ثغرات مدرجة من CVE-2026-117659 إلى CVE-2026-120298.
- درجة CVSS v3 المذكورة هي 8.1.
- تشمل أنواع الضعف التحقق غير السليم من الشهادات ومفتاح تشفير مضمّنًا في الشيفرة وغياب المصادقة لوظيفة حرجة.
- يحدد التنبيه قطاع المياه والصرف الصحي، مع انتشار المنتج عالميًا.

أصدرت CISA تنبيهًا يخص أنظمة التحكم الصناعي بشأن InfoScan، وهو منتج من شركة Dorsett Controls التي يقع مقرها في الولايات المتحدة. يشمل التنبيه الإصدارات حتى 1.45.0 ضمنًا، ويدرج ست ثغرات برقم CVE.

ما يذكره التنبيه

وفق التنبيه، قد يتيح الاستغلال الناجح للمهاجم الحصول على معلومات حساسة عن النظام، أو الوصول إلى بيانات التطبيق دون تصريح، أو استرجاع بيانات اعتماد مخزّنة، أو اعتراض الاتصالات الشبكية والتلاعب بها. ودرجة CVSS v3 المذكورة هي 8.1.

ومن فئات الضعف المذكورة: التحقق غير السليم من الشهادات، وكشف معلومات حساسة للنظام لجهة غير مصرّح لها، واستخدام مفتاح تشفير مضمّن في الشيفرة، وغياب المصادقة لوظيفة حرجة، ورسائل خطأ تتضمن معلومات حساسة. ومن الأمثلة الموصوفة أن عميل سطح المكتب InfoScan المبني على Electron يقبل شهادات TLS دون التحقق من موثوقيتها.

يحدد التنبيه قطاع أنظمة المياه والصرف الصحي بوصفه القطاع الحيوي المعني، مع انتشار المنتج حول العالم.

الخطوات التالية

لا يتضمن المقتطف الذي راجعناه إصلاحات من الشركة المصنّعة أو خطوات تخفيف. ينبغي للمشغّلين قراءة تنبيه CISA كاملاً وأي إرشادات من الشركة قبل تحديد المعالجة. وفي الأثناء، تحقّقوا من وجود InfoScan في بيئتكم ومن الإصدار المستخدم، وراجعوا كيفية إتاحة العملاء والخوادم على الشبكة.

ما يجب فعله الآن

1. راجعوا سجلات الأصول بحثًا عن InfoScan ودوّنوا الإصدارات المثبّتة.
2. اقرؤوا تنبيه CISA كاملاً وأي إرشادات من Dorsett Controls بشأن الإصلاحات أو التخفيف.
3. قيّدوا الوصول الشبكي إلى أنظمة InfoScan وأبقوها معزولة عن الشبكات المؤسسية.
4. اعتبروا بيانات الاعتماد المخزّنة أو المستخدمة في InfoScan معرّضة للكشف، وخطّطوا لتغييرها عند وجود إصدارات متأثرة.
5. راقبوا أي نشاط شبكي غير معتاد يخص الأجهزة التي تشغّل InfoScan.