CISA تحذّر من ثغرة إرسال بيانات حساسة بنص واضح في وحدات التحكم EasyIO Neo من Johnson Controls



نشرت CISA تنبيهاً بشأن الثغرة CVE-2026-64893 في وحدات EasyIO Neo من Johnson Controls، إذ قد تُرسل بيانات حساسة منها بيانات الاعتماد والجلسات بنص واضح يمكن لمهاجم على الشبكة قراءتها.

- تحمل الثغرة المعرّف CVE-2026-64893 وتُصنَّف إرسالًا لمعلومات حساسة بنص واضح.
- درجة CVSS v3 هي 5.4.
- الإصدارات المتأثرة: وحدات EC الإصدارات V3.3b62 وV3.3b63، ووحدات CW الإصدارات V3.3b24 وV3.3b25.
- يمكن لمهاجم قادر على اعتراض حركة الشبكة قراءة بيانات الاعتماد وبيانات الجلسات.
- تشمل القطاعات المذكورة التصنيع الحيوي والمرافق التجارية والمرافق الحكومية والنقل والطاقة.

نشرت CISA تنبيهاً خاصاً بأنظمة التحكم الصناعي يتناول وحدات التحكم EasyIO Neo Series EC وCW من Johnson Controls. وتتعلق الثغرة CVE-2026-64893 بإرسال معلومات حساسة بنص واضح عبر الشبكة.

ما الذي يقوله التنبيه

تفيد Johnson Controls بعلمها بأن مهاجماً قد يعترض معلومات مرسلة دون تشفير ويقرؤها، ومنها بيانات الاعتماد وبيانات الجلسات. وقد صُنّفت الثغرة بدرجة 5.4 وفق CVSS v3.

الإصدارات المتأثرة:

- وحدات EasyIO Neo Series EC الإصداران V3.3b62 وV3.3b63
- وحدات EasyIO Neo Series CW الإصداران V3.3b24 وV3.3b25

وتربط CISA المنتج بقطاعات التصنيع الحيوي والمرافق التجارية والخدمات والمرافق الحكومية وأنظمة النقل والطاقة. ومقر الشركة في أيرلندا، وتنتشر منتجاتها حول العالم.

أهمية الأمر

درجة الخطورة متوسطة، لكن حصول مهاجم على بيانات اعتماد أو جلسات قد يمنحه موطئ قدم في أنظمة التحكم بالمباني والمرافق. ويتوقف التعرض على إمكانية وصول المهاجم إلى مسار الشبكة بين المستخدمين ووحدات التحكم.

الخطوات التالية

ينبغي للجهات أولًا تحديد ما إذا كانت هذه الوحدات موجودة لديها وأي إصدارات تعمل عليها، ثم اتباع إرشادات المورّد وتنبيه CISA للمعالجة، ومراجعة طريقة الوصول إلى الوحدات عبر الشبكة. ولا يذكر المصدر المتاح تصحيحاً أو حلًا بديلًا، لذا يُستحسن التأكد من أحدث الإرشادات مباشرة من Johnson Controls.

ما يجب فعله الآن

1. حصر وحدات EasyIO Neo EC وCW وتسجيل إصدارات البرمجيات الثابتة ومقارنتها بقائمة الإصدارات المتأثرة.
2. مراجعة إرشادات Johnson Controls وتنبيه CISA بشأن المعالجة الحالية وتطبيقها.
3. حصر الوصول الشبكي إلى الوحدات في شبكات إدارة معزولة ومضيفين موثوقين فقط.
4. تغيير بيانات الاعتماد المستخدمة على الوحدات المتأثرة إذا كان تعرضها عبر شبكة غير موثوقة محتملًا.
5. مراقبة حركة الشبكة من الوحدات وإليها بحثاً عن جلسات أو عمليات دخول غير متوقعة.