

أجهزة التحكم في المباني Johnson Controls EasyIO FG تحتوي على ثغرات في بيانات الاعتماد المشفرة وإدارة الصلاحيات



حذرت وكالة الأمن السيبراني الأمريكي من أن أجهزة التحكم الآلي للمباني Johnson Controls EasyIO FG تحتوي على ثغرات في بيانات الاعتماد المشفرة وإدارة الصلاحيات قد تؤدي إلى اختراق كامل للجهاز.

- ثغرتان (CVE-2026-27872 و CVE-2026-27873) تؤثران على إصدار البرنامج الثابت EasyIO FG 2.0b52 والإصدارات الأقدم
- بيانات الاعتماد المشفرة وإدارة الصلاحيات غير الصحيحة قد تتيح وصولاً غير مصرح به بشكل كامل للجهاز
- درجة CVSS البالغة 7.7 تشير إلى تأثير عالي الخطورة على بيئات تقنية العمليات
- أعلنت Johnson Controls انتهاء عمر سلسلة EasyIO FG دون خطط لإصدار تحديثات أمنية
- الأنظمة المتأثرة منتشرة في قطاعات التصنيع الحرج والمنشآت التجارية والخدمات الحكومية

نظرة عامة على الثغرات

أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية تنبيهاً بشأن ثغرتين في أجهزة التحكم الآلي للمباني Johnson Controls EasyIO FG. الثغرتان المسجلتان برقم CVE-2026-27872 و CVE-2026-27873 تؤثران على جميع إصدارات البرنامج الثابت حتى الإصدار 2.0b52 وما قبله. تتبع كلتا الثغرتين من استخدام بيانات اعتماد مشفرة وإدارة صلاحيات غير صحيحة، مما يتيح للمهاجم الحصول على وصول كامل غير مصرح به للأجهزة المتأثرة. أعطت الوكالة درجة CVSS قدرها 7.7، مما يعكس احتمالية تأثير تقني وتشغيلي كبير.

سلسلة EasyIO FG منتشرة عالمياً عبر قطاعات البنية التحتية الحرجة بما في ذلك التصنيع الحرج والمنشآت التجارية والخدمات الحكومية وأنظمة النقل والطاقة. تدير أجهزة التحكم الآلي هذه أنظمة التدفئة والتهوية والإضاءة وأنظمة المنشآت الأخرى، مما يجعلها أهدافاً جذابة للخصوم الذين يسعون لتعطيل العمليات أو إنشاء موطئ قدم في بيئات تقنية العمليات.

حالة انتهاء العمر وعدم توفر تحديثات

قررت Johnson Controls EasyIO FG أن سلسلة قد وصلت إلى حالة انتهاء العمر. ونتيجة لذلك، لن تصدر الشركة تحديثات أمنية لمعالجة هذه الثغرات. تواجه المؤسسات التي تعتمد على هذه الأجهزة خياراً بين قبول المخاطر أو تطبيق ضوابط تعويضية أو استبدال الأجهزة المتأثرة ببدائل مدعومة.

المخاطر على المؤسسات السعودية الخاضعة للتنظيم

بالنسبة للمؤسسات العاملة بموجب أطر الهيئة الوطنية للأمن السيبراني أو لوائح مؤسسة النقد العربي السعودي، فإن وجود ثغرات غير مصححة في بيئات تقنية العمليات يمثل مخاطر على الامتثال والعمليات. غالباً ما تربط أنظمة التحكم الآلي في المباني بين شبكات تقنية المعلومات وتقنية العمليات، وقد يوفر اختراق هذه الأجهزة للمهاجمين فرص التنقل الجانبي أو تمكين تعطيل العمليات الحرجة للمنشآت.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع أجهزة التحكم Johnson Controls EasyIO FG عبر منشآتكم وتوثيق إصدارات البرامج الثابتة
2. عزل الأجهزة المتأثرة على شرائح شبكية مخصصة مع قواعد جدار حماية صارمة تمنع الوصول المباشر للإنترنت وتحد من التنقل الجانبي
3. تطبيق مراقبة وتسجيل معززين لجميع أجهزة EasyIO FG لاكتشاف محاولات الوصول غير المصرح بها أو تغييرات التكوين
4. تطوير وتنفيذ خارطة طريق لاستبدال أجهزة التحكم EasyIO FG منتهية العمر، مع إعطاء الأولوية للأجهزة في البنية التحتية الحرجة أو المناطق عالية الأمان
5. مراجعة وتحديث ضوابط أمن أنظمة التحكم الآلي في المباني بما يتماشى مع متطلبات الإطار الوطني للأمن السيبراني لتقنية العمليات الصادر عن الهيئة الوطنية للأمن السيبراني

6. إحاطة فرق إدارة المنشآت وتقنية العمليات بالثغرة والتدابير الأمنية المؤقتة حتى اكتمال الاستبدال