

Inductive Automation Ignition: ثغرة رفع صلاحيات (CVE-2026-92817) تتيح تنفيذ تعليمات برمجية



أصدرت CISA نشرة عن ثغرة تحقق صلاحيات في CVSS 8.8 (CVE-2026-92817 Ignition) تتيح لمستخدم موثّق محدود الصلاحيات الحصول على صلاحيات Designer وتنفيذ تعليمات على Gateway. تشمل الإصدارات 8.1.0-8.1.54 و8.3.0-8.3.8.

- CVE-2026-92817 ثغرة تحقق صلاحيات غير سليم بدرجة CVSS v3 تبلغ 8.8.
- الإصدارات المتأثرة: Ignition من 8.1.0 إلى 8.1.54 ومن 8.3.0 إلى 8.3.8.
- وحدة Perspective لا تتحقق جيداً من صلاحيات الجلسة عند تحديد الوصول بمستوى Designer.
- يمكن لمستخدم لديه وصول إلى مشروع Vision استخدام معرفّ جلسة Vision صالح للحصول على صلاحيات Designer.
- قد يتيح الاستغلال تنفيذ تعليمات برمجية عشوائية ضمن عملية Ignition Gateway.

نشرت CISA نشرة تخص أنظمة التحكم الصناعي بشأن برنامج Inductive Automation Ignition، وهو منصة صناعية تُستخدم عالمياً في قطاعات التصنيع الحيوي والطاقة وتقنية المعلومات.

طبيعة الثغرة

الثغرة المسجلة برقم **CVE-2026-92817** هي ضعف في التحقق من الصلاحيات بدرجة 8.8 وفق مقياس CVSS v3. فوحدة Ignition Perspective لا تتحقق على نحو سليم من صلاحيات الجلسة عند تحديد ما إذا كان للمستخدم وصول بمستوى Designer. ويمكن للمستخدم موثق لديه وصول إلى مشروع Vision أن يقدم معرف جلسة Vision صالحاً خاصاً به فيحصل على صلاحيات Designer.

وبهذه الصلاحيات المرتفعة قد يتمكن المهاجم من تنفيذ تعليمات برمجية عشوائية ضمن عملية Ignition Gateway.

الإصدارات المتأثرة

- Ignition من 8.1.0 إلى 8.1.54
- Ignition من 8.3.0 إلى 8.3.8

تشير النشرة إلى أن Inductive Automation أصدرت الإصدار 8.3.9 كإجراء معالجة. ولا يتضمن المقتطف تفاصيل إضافية للمعالجة، لذا ينبغي الرجوع إلى نشرة CISA الكاملة وإلى إرشادات الشركة المصنعة.

الأثر على الجهات المشغلة

يتطلب الاستغلال تسجيل دخول صالحاً، ولذلك يرتبط التعرض بمن يملك حسابات ذات وصول إلى مشاريع Vision. وعلى الجهات التي تشغل Ignition في بيئاتها التشغيلية تحديد إصداراتها، ومراجعة المستخدمين الذين يصلون إلى مشاريع Vision، والتخطيط للتحديث عبر إجراءات إدارة التغيير المعتمدة لأنظمة التقنية التشغيلية.

ما يجب فعله الآن

1. حصر جميع أنظمة Ignition وتحديد أي إصدارات من 8.1.0 إلى 8.1.54 أو من 8.3.0 إلى 8.3.8.
2. مراجعة نشرة CISA الكاملة وإرشادات Inductive Automation، ثم التخطيط للتحديث إلى إصدار مُعالج مثل 8.3.9 عبر إدارة التغيير في بيئة التقنية التشغيلية.
3. مراجعة الحسابات ذات الوصول إلى مشاريع Vision وإزالة الوصول غير الضروري.
4. مراقبة خوادم Ignition Gateway لرصد أي نشاط غير متوقع بمستوى Designer أو سلوك غير معتاد للعمليات.
5. توثيق حالة التعرض والمعالجة في سجل مخاطر التقنية التشغيلية بما يتوافق مع ضوابط الأمن السيرياني للأنظمة التشغيلية (NCA OTCC).