Moxa AIG-302 ThingsPro Edge: ثغرتان قد تكشفان معلومات حساسة ومفاتيح تشفير



نشرت CISA تنبيهاً عن ثغرتين في البرنامج الثابت لجهاز Moxa AIG-302 ThingsPro Edge حتى الإصدار 1.4.0، بتقييم CVSS v3 قدره 8.1. قد يتيح الاستغلال كشف معلومات حساسة، وقد وفّرت Moxa إصلاحاً.

- المتأثر: البرنامج الثابت لجهاز Moxa AIG-302 ThingsPro Edge بالإصدار 1.4.0 والإصدارات الأقدم.
- ثغرتان: CVE-2026-109812 وCVE-2026-109813، تتعلقان بغياب التحقق من الصلاحيات واستخدام مفتاح تشفير مضمّن في الشيفرة.
- تقييم CVSS v3 هو 8.1، والأثر هو كشف معلومات حساسة.
- الثغرة CVE-2026-109812 تخص واجهة API الداخلية /api/v1/secrets/ وتتطلب مهاجماً مصادَقاً بصلاحيات مرتفعة ولديه وصول من شبكة مجاورة.
- وفّرت Moxa إصلاحاً؛ والقطاعات المذكورة هي التصنيع الحيوي والطاقة والمياه والصرف الصحي.

أصدرت CISA تنبيهاً خاصاً بأنظمة التحكم الصناعي بشأن ثغرتين في البرنامج الثابت لجهاز Moxa AIG-302 ThingsPro Edge. وتشمل الإصدارات المتأثرة كل ما هو حتى 1.4.0 ضمناً. ويحدد التنبيه تقييم CVSS v3 بقيمة 8.1، ويشير إلى أن الاستغلال الناجح قد يمكّن المهاجم من الحصول على معلومات حساسة وكشفها.

ما الذي يقوله التنبيه

الثغرتان هما CVE-2026-109812 وCVE-2026-109813، وتوصفان بأنهما **غياب التحقق من الصلاحيات** و**استخدام مفتاح تشفير مضمّن في الشيفرة**.

في CVE-2026-109812 يكمن الخلل في واجهة API الداخلية /api/v1/secrets/. وقد يستغله مهاجم مصادَق بصلاحيات مرتفعة ولديه وصول من شبكة مجاورة للوصول إلى معلومات حساسة، منها مواد مفاتيح التشفير. أما تفاصيل CVE-2026-109813 فلم ترد في المقتطف الذي اطلعنا عليه.

مقر Moxa في تايوان، وتنتشر منتجاتها حول العالم. وتذكر CISA من القطاعات المعنية التصنيع الحيوي والطاقة وأنظمة المياه والصرف الصحي. وتشير إلى أن Moxa وفّرت إصلاحاً.

ما يعنيه ذلك للمشغّلين

الشروط المذكورة، وهي الصلاحيات المرتفعة والموقع في شبكة مجاورة، تحدّ من مسارات الهجوم المحتملة، لكنها لا تلغي الخطر إذا كانت شبكات الإدارة أو التشغيل ضعيفة العزل. كما أن تسرّب مواد المفاتيح قد يمتد أثره إلى ما وراء الجهاز نفسه، لذا ينبغي التعامل مع الأمر كمسألة إدارة بيانات اعتماد إلى جانب كونه تحديثاً برمجياً.

على الجهات أولًا التأكد من وجود هذه الأجهزة في بيئتها، ثم اتباع إرشادات المورّد للمعالجة.

ما يجب فعله الآن

1. حصر أجهزة Moxa AIG-302 ThingsPro Edge في بيئات التقنية التشغيلية والحوسبة الطرفية وتسجيل إصدارات البرنامج الثابت.
2. تطبيق الإصلاح الذي وفّرته Moxa على أي جهاز يعمل بالإصدار 1.4.0 أو أقدم، وفق إجراءات إدارة التغيير والاختبار.
3. تقييد الوصول من الشبكات المجاورة إلى هذه الأجهزة عبر العزل الشبكي، وحصر الحسابات ذات الصلاحيات المرتفعة.
4. تقييم الحاجة إلى تدوير المفاتيح أو الأسرار المخزنة على الأجهزة المتأثرة أو المستخدمة فيها بعد التحديث.
5. توثيق حالة التعرض والمعالجة في سجل مخاطر التقنية التشغيلية ورفعها ضمن حوكمة أمن التقنية التشغيلية الداخلية.