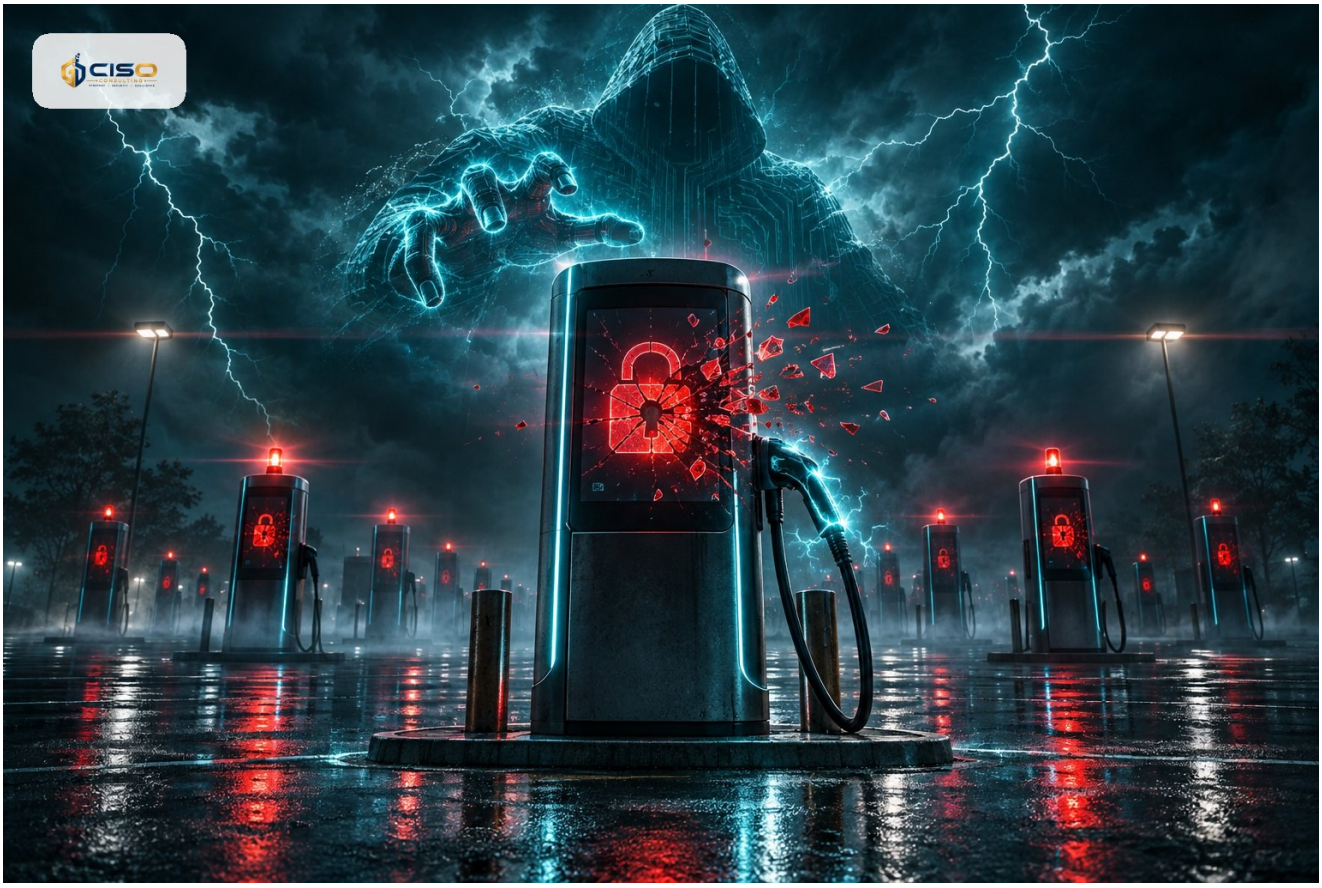
CISA تحذّر من ثغرات حرجة في منصة شحن المركبات الكهربائية Monta monta.app



نشرت CISA تنبيهاً لأنظمة التحكم الصناعي بشأن Monta monta.app يشمل أربع ثغرات (CVSS v3 بدرجة 9.4) قد تمنح المهاجم تحكماً إدارياً بمحطات الشحن أو تعطّل الخدمة. وتشمل جميع الإصدارات.

- أربع ثغرات تؤثر على جميع إصدارات Monta monta.app: CVE-2026-95102 وCVE-2026-97363 وCVE-2026-97212 وCVE-2026-93474.
- درجة CVSS v3 هي 9.4.
- أنواع الضعف: غياب المصادقة لوظيفة حرجة، وعدم تقييد محاولات المصادقة المفرطة، وعدم كفاية انتهاء الجلسات، وضعف حماية بيانات الاعتماد.
- الثغرة CVE-2026-95102: نقاط WebSocket بلا مصادقة، ما يتيح انتحال هوية محطات الشحن.
- الأثر: تحكم إداري غير مصرح به بالمحطات أو حجب الخدمة. القطاعان المذكوران: الطاقة وأنظمة النقل.

أصدرت CISA تنبيهاً لأنظمة التحكم الصناعي بشأن monta.app، وهو منتج إدارة الشحن من شركة Monta التي يقع مقرها في هولندا. يغطي التنبيه أربع ثغرات بدرجة 9.4 وفق مقياس CVSS v3، ويذكر المصدر أن جميع الإصدارات متأثرة.

ما الذي يوضحه التنبيه

تتمثل نقاط الضعف في غياب المصادقة لوظيفة حرجة، وعدم تقييد محاولات المصادقة المفرطة، وعدم كفاية انتهاء الجلسات، وضعف حماية بيانات الاعتماد. وهي مسجلة بالأرقام CVE-2026-95102 وCVE-2026-97363 وCVE-2026-97212 وCVE-2026-93474.

ففي الثغرة CVE-2026-95102 لا تتحقق نقاط WebSocket من هوية الجهة المتصلة بها. وقد ينتحل المهاجم هوية محطة شحن، ويصل إلى بيانات حساسة أو ينفذ إجراءات غير مصرح بها، ولأن المصادقة غير مطلوبة فقد يؤدي ذلك إلى رفع الصلاحيات على مستوى المنظومة. ولا يوضح المقتطف المتاح تفاصيل الثغرات الثلاث الأخرى.

وتفيد CISA بأن الاستغلال الناجح قد يمنح المهاجمين تحكماً إدارياً غير مصرح به بمحطات الشحن المعرضة، أو يمكّنهم من تعطيل خدمات الشحن عبر هجمات حجب الخدمة. ويذكر التنبيه قطاعي الطاقة وأنظمة النقل، وانتشار المنتج حول العالم.

الأهمية للجهات في المملكة

ينبغي للجهات التي تشغّل بنية شحن المركبات الكهربائية أو تستضيفها، أو تعتمد على مزود يستخدم هذه المنصة، أن تتحقق من وجود monta.app في بيئتها. ولا يذكر المقتطف وجود تحديث أو معالجة، لذا يُرجع إلى تنبيه CISA الكامل وإلى المورّد للحصول على أحدث إرشادات التخفيف.

ما يجب فعله الآن

1. تحقق مما إذا كان monta.app مستخدماً في بنية الشحن لديكم أو لدى مزودي خدمات الشحن.
2. اطلعوا على تنبيه CISA الكامل وتواصلوا مع Monta أو مزودكم للحصول على التحديثات وإرشادات التخفيف.
3. قيّدوا إتاحة منصات إدارة الشحن ونقاط WebSocket على الشبكة بحيث تقتصر على المصادر الموثوقة.
4. راقبوا تسجيل المحطات غير المتوقع والإجراءات الإدارية ومحاولات المصادقة المتكررة.
5. راجعوا مدد الجلسات وطريقة تخزين بيانات الاعتماد لحسابات إدارة الشحن.
6. أدرجوا هذا التعرض في سجل مخاطر التقنية التشغيلية وواءموا الاستجابة مع ضوابط الأمن السيبراني للأنظمة التشغيلية (NCA OTCC).