سلسلة Hitachi Energy TRO600: ثغرتان قد تتيحان تنفيذ تعليمات برمجية عن بُعد وكشف بيانات حساسة



نشرت CISA إشعارًا بشأن ثغرتين في منتجات Hitachi Energy من سلسلة TRO600 قد تتيحان تنفيذ تعليمات برمجية عن بُعد وكشف معلومات حساسة. وقدّرت الشركة الخطورة بـ 7.5 وفق CVSS v3.

- تؤثر الثغرتان CVE-2026-10756 وCVE-2026-106087 في سلسلة TRO600.
- تشمل الإصدارات المتأثرة TRO600 حتى 9.2.1.6 وحتى 9.1.1.0، إضافةً إلى 9.2.2.1 و9.1.2.0.
- نوع الضعف: تقييد غير سليم لقنوات الاتصال، وغياب المصادقة لوظيفة حرجة.
- تتيح CVE-2026-10756 لمهاجم موثّق تجاوز قيود الشبكة والوصول إلى خدمات مخصصة للمضيف المحلي فقط عبر تمرير المنافذ.
- قدّرت الشركة الخطورة بـ 7.5 وفق CVSS v3، والقطاع المعني هو الطاقة مع انتشار عالمي.

نشرت CISA إشعارًا خاصًا بأنظمة التحكم الصناعي يتناول منتجات Hitachi Energy من سلسلة TRO600. ووفق الإشعار، يمكن استغلال الثغرات لتنفيذ تعليمات برمجية عن بُعد تمهيدًا لهجمات لاحقة، ولكشف معلومات حساسة.

ما الذي تأثر

أُدرجت ثغرتان: CVE-2026-10756 وCVE-2026-106087. والإصدارات المتأثرة هي TRO600 حتى 9.2.1.6، وحتى 9.1.1.0، إضافةً إلى الإصدارين 9.2.2.1 و9.1.2.0. وتمنح الشركة الثغرات درجة 7.5 وفق CVSS v3. أما نوع الضعف فهو تقييد غير سليم لقنوات الاتصال نحو الجهات المقصودة، وغياب المصادقة لوظيفة حرجة.

وفي CVE-2026-10756، يستطيع مهاجم موثّق تجاوز قيود الوصول إلى الشبكة والوصول إلى خدمات يُفترض أن تكون متاحة من المضيف المحلي فقط. وعبر تمرير المنافذ يمكنه التفاعل مع المنافذ والخدمات المرتبطة محليًا.

السياق

يصنّف الإشعار المنتجات ضمن قطاع الطاقة، وهي منتشرة عالمًا، ومقر الشركة في سويسرا. ولا يذكر المقتطف المنشور وجود استغلال فعلي، لذا يُعامل الأمر كمهمة معالجة ومراجعة تعرّض لا كحالة طوارئ.

النهج الموصى به

توجّه Hitachi Energy المستخدمين إلى قسم الإجراءات الفورية الموصى بها في الإشعار للتخفيف والمعالجة. وينبغي للمشغّلين التحقق من وجود أجهزة TRO600 لديهم، وتحديد إصدارات البرمجيات الثابتة، واتباع إرشادات المورّد.

ما يجب فعله الآن

1. حصر أجهزة TRO600 في المواقع التشغيلية والبعيدة وتوثيق إصدارات البرمجيات الثابتة.
2. مطابقة الإصدارات مع القائمة المتأثرة وتطبيق الإجراءات الفورية الموصى بها من المورّد.
3. تقييد الوصول إلى واجهات إدارة الأجهزة والحد من الحسابات القادرة على المصادقة عليها.
4. مراجعة السجلات بحثًا عن تمرير منافذ غير متوقع أو اتصالات بخدمات محلية على هذه الأجهزة.
5. تسجيل الملاحظة في سجل مخاطر التقنية التشغيلية والإبلاغ وفق ضوابط NCA OTCC والإجراءات الداخلية عند الاقتضاء.