

Hitachi Energy RTU500: تنبيه من CISA بشأن ثغرات متعددة في البرنامج الثابت لوحدة CMU



نشرت CISA تنبيهاً عن ثغرات في البرنامج الثابت لوحدة CMU ضمن سلسلة RTU500 من Hitachi Energy، وقد يؤثر استغلالها على السرية والسلامة والتوافر. يُنصح المشغّلون بمراجعة الإصدارات المتأثرة.

- يشمل التنبيه البرنامج الثابت لوحدة CMU في سلسلة RTU500 من Hitachi Energy.
- النطاقات المتأثرة: 12.7.1-13.5.4 و 13.6.1-13.6.3 و 13.7.1-13.7.8 و 13.8.1-13.8.2.
- من الثغرات المدرجة: CVE-2026-17539 و CVE-2026-28388 و CVE-2026-6732 و CVE-2026-6653 و CVE-2026-6276 وغيرها.
- قد يؤثر الاستغلال على سرية المنتج وسلامته وتوافره.
- تُحيل الجهة المصنّعة إلى «الإجراءات الفورية الموصى بها» للمعالجة والتخفيف.

ما الذي نُشر

أصدرت CISA تنبيهًا يخص أنظمة التحكم الصناعي بشأن منتجات سلسلة RTU500 من Hitachi Energy. وتفيد الشركة بأنها على علم بثغرات في البرنامج الثابت لوحدة CMU قد يؤدي استغلالها إلى التأثير على سرية المنتج وسلامته وتوافره.

والنطاقات المتأثرة من البرنامج الثابت هي: من 12.7.1 إلى 12.7.7، ومن 13.5.1 إلى 13.5.4، ومن 13.6.1 إلى 13.6.3، ومن 13.7.1 إلى 13.7.8، ومن 13.8.1 إلى 13.8.2. ويورد التنبيه عدة ثغرات منها CVE-2026-17539 و CVE-2026-28388 و CVE-2026-6732 و CVE-2026-6653 و CVE-2026-6276 و CVE-2026-9079 و CVE-2026-11856 و CVE-2026-8927 و CVE-2026-8932.

ما لا يذكره المصدر

لا يتضمن المقتطف المتاح لنا درجات الخطورة ولا التفاصيل التقنية لكل ثغرة، ولا أي إشارة إلى استغلالها فعليًا. لذلك لا نجزم في هذه النقاط، ويبقى التنبيه الكامل وإرشادات الجهة المصنّعة «الإجراءات الفورية الموصى بها» هما المرجع المعتمد.

نهج مقترح

على الجهات التي تشغّل أجهزة RTU500، مثل شركات المرافق ومشغّلي البنية التحتية الحرجة، التحقق أولاً مما إذا كان إصدار البرنامج الثابت لوحدة CMU لديها ضمن النطاقات المذكورة، ثم تطبيق إرشادات المعالجة والتخفيف الصادرة عن الجهة المصنّعة عبر إجراءات إدارة التغيير المعتمدة في بيئة التقنية التشغيلية.

ما يجب فعله الآن

1. حصر جميع وحدات RTU500 وتسجيل إصدارات البرنامج الثابت لوحدة CMU ومقارنتها بالنطاقات المتأثرة.
2. الاطلاع على تنبيه CISA كاملاً وعلى «الإجراءات الفورية الموصى بها» من Hitachi Energy، ثم التخطيط للمعالجة أو التخفيف.
3. جدولة المعالجة ضمن إدارة التغيير في بيئة التقنية التشغيلية مع الاختبار وخطة للتراجع.
4. مراجعة تعرّض أجهزة RTU500 للشبكات والتأكد من وجودها في مناطق تشغيلية معزولة.
5. رفع تقرير بالأصول المتأثرة وحالة المعالجة إلى مالك مخاطر التقنية التشغيلية وفق ضوابط الأمن السيرياني للأنظمة التشغيلية (NCA OTCC).