Hitachi Energy REB500 حتى الإصدار 8.3.3.1: ثغرات في مكوّنات مفتوحة المصدر قد تتسبب في حجب الخدمة



أصدرت CISA نشرة بشأن ثغرتين في مكتبات مفتوحة المصدر (CVE-2024-8176 وCVE-2025-59375) في REB500 من Hitachi Energy حتى الإصدار 8.3.3.1، قد تتيح حجب الخدمة. يُنصح بمراجعة إجراءات المورّد.

- المنتج المتأثر: REB500 من Hitachi Energy بإصداراته حتى 8.3.3.1 وما قبلها.
- ثغرتان: CVE-2024-8176 وCVE-2025-59375، في مكوّنات برمجية مفتوحة المصدر.
- الأثر: حجب الخدمة، وفي بعض البيئات قد يحدث تلف في الذاكرة بالنسبة إلى CVE-2024-8176.
- CVE-2024-8176 فيض في المكدس (stack overflow) في مكتبة libexpat المستخدمة في وظائف IEC 61850، ويُستغل برسالة مصممة من مستخدم موثّق لديه وصول محلي.
- درجة CVSS v3 لدى المورّد 6.5، والمنتج مستخدم في قطاع الطاقة حول العالم.

نشرت CISA نشرة استشارية بشأن منتج REB500 من Hitachi Energy، تتناول ثغرات في مكوّنات برمجية مفتوحة المصدر يتضمنها. وتفيد الشركة بأن هذه الثغرات قد تُستغل لتنفيذ هجوم حجب خدمة ضد المنتج.

ما الذي يتأثر

تشمل الإصدارات المتأثرة جميع إصدارات REB500 حتى 8.3.3.1 وما قبلها. وتذكر النشرة ثغرتين هما CVE-2024-8176 وCVE-2025-59375، ويقدّر المورّد شدتهما بدرجة CVSS v3 قدرها 6.5. وتتعلق نوعا الضعف بالتكرار غير المضبوط (uncontrolled recursion) وتخصيص الموارد دون حدود أو تقييد.

أما CVE-2024-8176 ففيض في المكدس داخل مكتبة libexpat التي تعتمد عليها وظائف IEC 61850 في REB500. ويمكن لمستخدم موثّق لديه وصول محلي إرسال رسالة IEC 61850 مصممة لاستغلالها. وبحسب البيئة وطريقة استخدام المكتبة، قد تكون النتيجة حجب الخدمة، أو في بعض الحالات تلفاً في الذاكرة قابلًا للاستغلال.

كيف تُقرأ هذه النشرة

يتطلب مسار الهجوم الموصوف مصادقة ووصولًا محلياً، وهذا يحدّ من التعرض لكنه لا يلغيه حيث تكون الحسابات أو الوصول المحلي غير مضبوطين جيداً. وتحدد النشرة قطاع الطاقة بوصفه القطاع الحيوي المتأثر، وتشير إلى انتشار المنتج حول العالم.

الخطوات التالية

تحيل النشرة إلى «الإجراءات الفورية الموصى بها» لدى المورّد للتخفيف والمعالجة. وعلى المشغّلين تحديد وحدات REB500 لديهم، والتأكد من إصدارها، وتطبيق هذه الإرشادات عبر إجراءات إدارة التغيير المعتمدة لبيئات التقنية التشغيلية.

ما يجب فعله الآن

1. حصر جميع وحدات REB500 والتحقق مما إذا كان أي منها يعمل بالإصدار 8.3.3.1 أو أقدم.
2. الاطلاع على «الإجراءات الفورية الموصى بها» من Hitachi Energy وتخطيط التخفيف أو المعالجة للوحدات المتأثرة.
3. تقييد الوصول المحلي ومراجعة الحسابات الموثّقة على أجهزة REB500، لأن الاستغلال يتطلب الأمرين معاً.
4. تقييد حركة IEC 61850 الواصلة إلى الأجهزة المتأثرة ومراقبتها.
5. تسجيل حالة التعرض والمعالجة في سجل مخاطر التقنية التشغيلية وفق متطلبات ضوابط الأمن السيبراني للأنظمة التشغيلية (NCA OTCC).