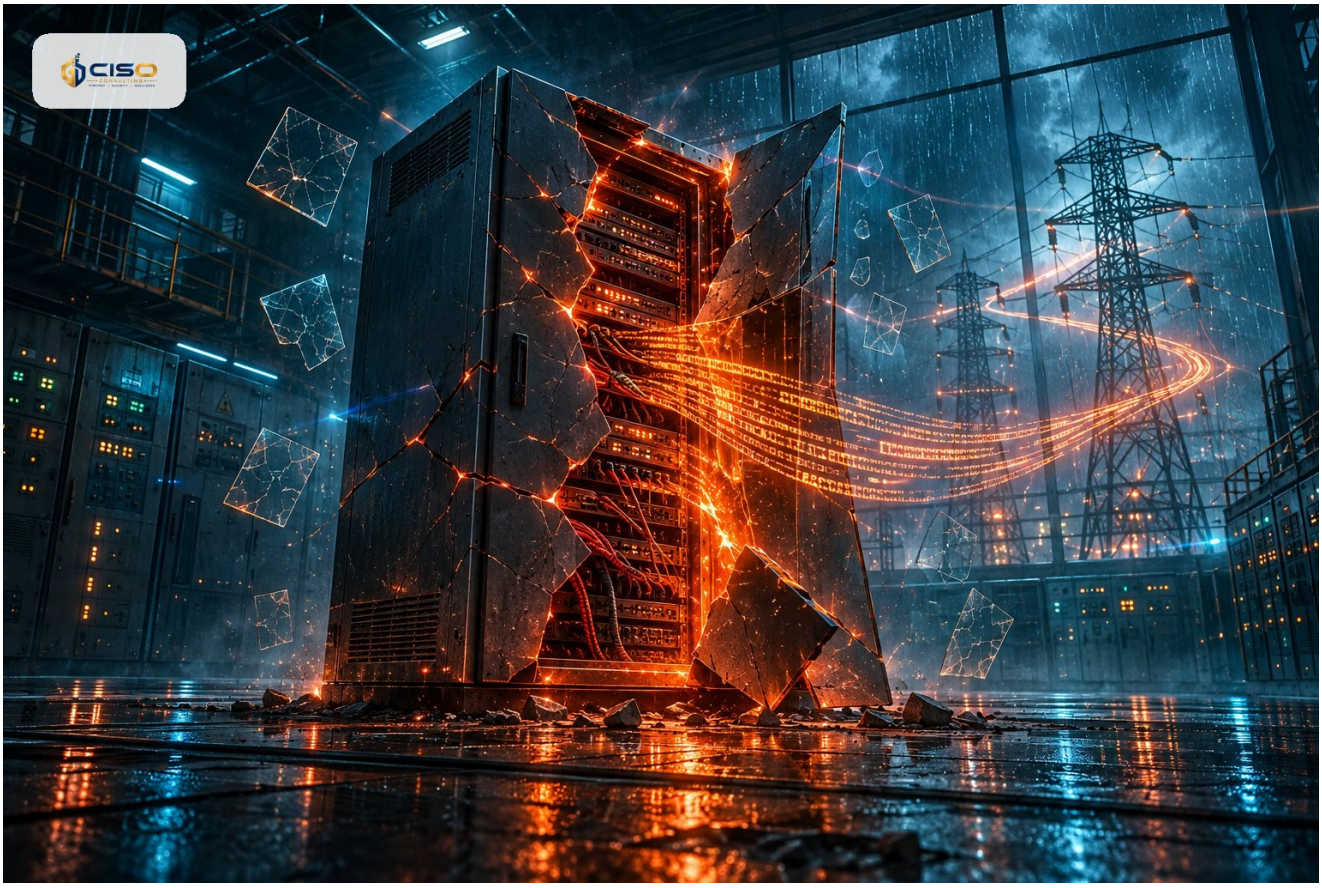
Hitachi Energy CoreTec: ثغرتان لحقن أوامر نظام التشغيل وDirty Frag



نشرت CISA نشرة بشأن ثغرتين في منتج Hitachi Energy CoreTec بإصداريه 4 و5، هما حقن أوامر نظام التشغيل وثغرة Dirty Frag، وقد يؤثر استغلالهما في سرية المنتج وسلامته وتوافره.

- الإصدارات المتأثرة: CoreTec5 حتى 3.4.0 والإصدار 5.0.0 (CVE-2026-13162 وCVE-2026-43284)، وCoreTec4 حتى 3.4.0 (CVE-2026-13162).
- تتيح CVE-2026-13162 لمستخدمين موثقين بأدوار معينة تنفيذ أوامر نظام عشوائية مع سيطرة كاملة على الجهاز.
- تقييم CVSS v3 الصادر عن المورد هو 8.8.
- الثغرة الثانية من نوع write-what-where ويُشار إليها بـ Dirty Frag.
- تُدرج النشرة قطاع الطاقة ضمن القطاعات المعنية، مع انتشار المنتج عالميًا.

ما الذي تم الإبلاغ عنه

أعادت CISA نشر نشرة من Hitachi Energy تخص منتجات CoreTec. وتصف النشرة ثغرتين: حقن أوامر نظام التشغيل (CVE-2026-13162)، وحالة write-what-where تُعرف باسم Dirty Frag (CVE-2026-43284).

تؤثر CVE-2026-13162 في CoreTec4 وCoreTec5، وتتيح لمستخدم موثق يملك أدوارًا معينة تنفيذ أوامر نظام عشوائية والسيطرة الكاملة على الجهاز. أما CVE-2026-43284 فمدرجة لـ CoreTec5 فقط.

الإصدارات المتأثرة

- CoreTec5: الإصدارات حتى 3.4.0، والإصدار 5.0.0
- CoreTec4: الإصدارات حتى 3.4.0

يقيّم المورد الثغرة بدرجة 8.8 وفق CVSS v3. وقد يؤثر الاستغلال الناجح في سرية المنتج وسلامته وتوافره. وتدرج النشرة المنتج ضمن قطاع الطاقة.

الأهمية للمنظمات

بما أن الاستغلال يتطلب حسابًا موثقًا بأدوار محددة، فإن ضبط الصلاحيات المميزة والتحكم في مسارات الشبكة إلى هذه الأجهزة عاملان أساسيان لتقليل التعرض. وينبغي للمشغلين مراجعة الإجراءات الفورية الموصى بها من المورد لمعرفة خطوات المعالجة الدقيقة.

ما يجب فعله الآن

1. حدد أجهزة CoreTec4 وCoreTec5 في بيئة التقنية التشغيلية وقارن إصداراتها بقائمة الإصدارات المتأثرة.
2. طبّق خطوات التخفيف والمعالجة الواردة في الإجراءات الفورية الموصى بها من المورد.
3. راجع الحسابات ذات الأدوار المرتفعة على هذه الأجهزة وأزل غير الضروري منها.
4. قيّد الوصول الشبكي إلى واجهات إدارة الأجهزة بحيث يقتصر على شرائح معتمدة.
5. وثّق التعرض في سجل مخاطر التقنية التشغيلية وفق ضوابط الأمن السيبراني للأنظمة التشغيلية (NCA OTCC).