

ثغرات في Hitachi Energy Asset Suite تسمح بالوصول غير المصادق عليه



أصدرت CISA تنبيهاً بشأن ثغرات حرجية في Hitachi Energy Asset Suite الإصدار 9.9.0 والإصدارات الأقدم تسمح بتجاوز المصادقة والوصول إلى خدمات الاختبار مما قد يؤثر على السرية والسلامة.

- ثغرتان أمنيّتان (CVE-2026-7395 و CVE-2026-11796) تؤثران على Asset Suite الإصدار 9.9.0 والإصدارات الأقدم
- يمكن للمستخدمين غير المصادق عليهم الوصول إلى HTTPPublishAdapterTestServlet المخصصة لبيئات الاختبار فقط
- قد يؤدي الاستغلال إلى رفع ملفات التكوين والكشف عن المعلومات والإضرار بسلامة البيانات
- درجة CVSS v3 البالغة 8.1 تشير إلى خطورة عالية مع تأثير محتمل على السرية والسلامة والتوافر
- تؤثر الثغرات على البنية التحتية لقطاع الطاقة المنتشرة عالمياً

نظرة عامة على الثغرات

أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية تنبيهاً بشأن ثغرات تجاوز المصادقة في Hitachi Energy Asset Suite. تؤثر الثغرات على جميع الإصدارات حتى 9.9.0 وتم تتبعها تحت الرقمين CVE-2026-7395 و CVE-2026-11796. بدرجة CVSS v3 قدرها 8.1، تمثل هذه الثغرات غياب المصادقة لوظيفة حرجية يمكن استغلالها من قبل جهات غير مصادق عليها.

تسمح الثغرة الرئيسية بالوصول غير المصرح به إلى HTTPPublishAdapterTestServlet، وهو مكون مصمم حصرياً للاختبار في بيئات غير إنتاجية. يمكن الاستغلال الناجح المهاجمين من رفع ملفات التكوين، مما قد يؤدي إلى الكشف عن المعلومات والإضرار بسلامة البيانات. تشكل الثغرات مخاطر على سرية وسلامة وتوافر الأنظمة المتأثرة.

التأثير على قطاع الطاقة

يتم نشر Asset Suite عالمياً ضمن قطاع الطاقة المصنف كبنية تحتية حرجية. يجب على المؤسسات التي تدير منشآت الطاقة أو المحطات الفرعية أو بيئات تقنية التشغيل ذات الصلة التي تستخدم هذه المنصة التعامل مع هذا التنبيه كأولوية عاجلة. أقر المورد السويسري بالثغرات وقدم إرشادات التخفيف.

إرشادات التخفيف

أصدرت Hitachi Energy إجراءات فورية موصى بها للنشرات المتأثرة. يجب على المؤسسات الرجوع إلى وثائق المعالجة الرسمية للمورد وتقييم ما إذا كانت خدمات الاختبار معرضة في البيئات الإنتاجية. ينبغي مراجعة تقسيم الشبكة وضوابط الوصول لضمان عزل مكونات الاختبار عن الشبكات التشغيلية.

ما يجب فعله الآن

1. جرد جميع نشرات Hitachi Energy Asset Suite ضمن بيئة تقنية التشغيل لديكم والتأكد من أرقام الإصدارات
2. مراجعة بنية الشبكة للتحقق من عدم إمكانية الوصول إلى HTTPPublishAdapterTestServlet ومكونات الاختبار المشابهة من الشبكات الإنتاجية
3. الرجوع إلى إرشادات المعالجة الرسمية من Hitachi Energy وتطبيق إجراءات التخفيف الموصى بها من المورد فوراً للإصدارات المتأثرة
4. تطبيق تقسيم الشبكة لعزل بيئات الاختبار والتطوير عن أنظمة التحكم التشغيلية
5. مراقبة سجلات الوصول للكشف عن نشاط غير اعتيادي يستهدف نقاط servlet، خاصة محاولات الوصول غير المصادق عليها
6. التنسيق مع فريق أمن تقنية التشغيل لجدولة التحديثات أو الضوابط التعويضية وفقاً لمتطلبات إدارة التغيير في الإطار الوطني للضوابط الأساسية لأمن تقنية التشغيل