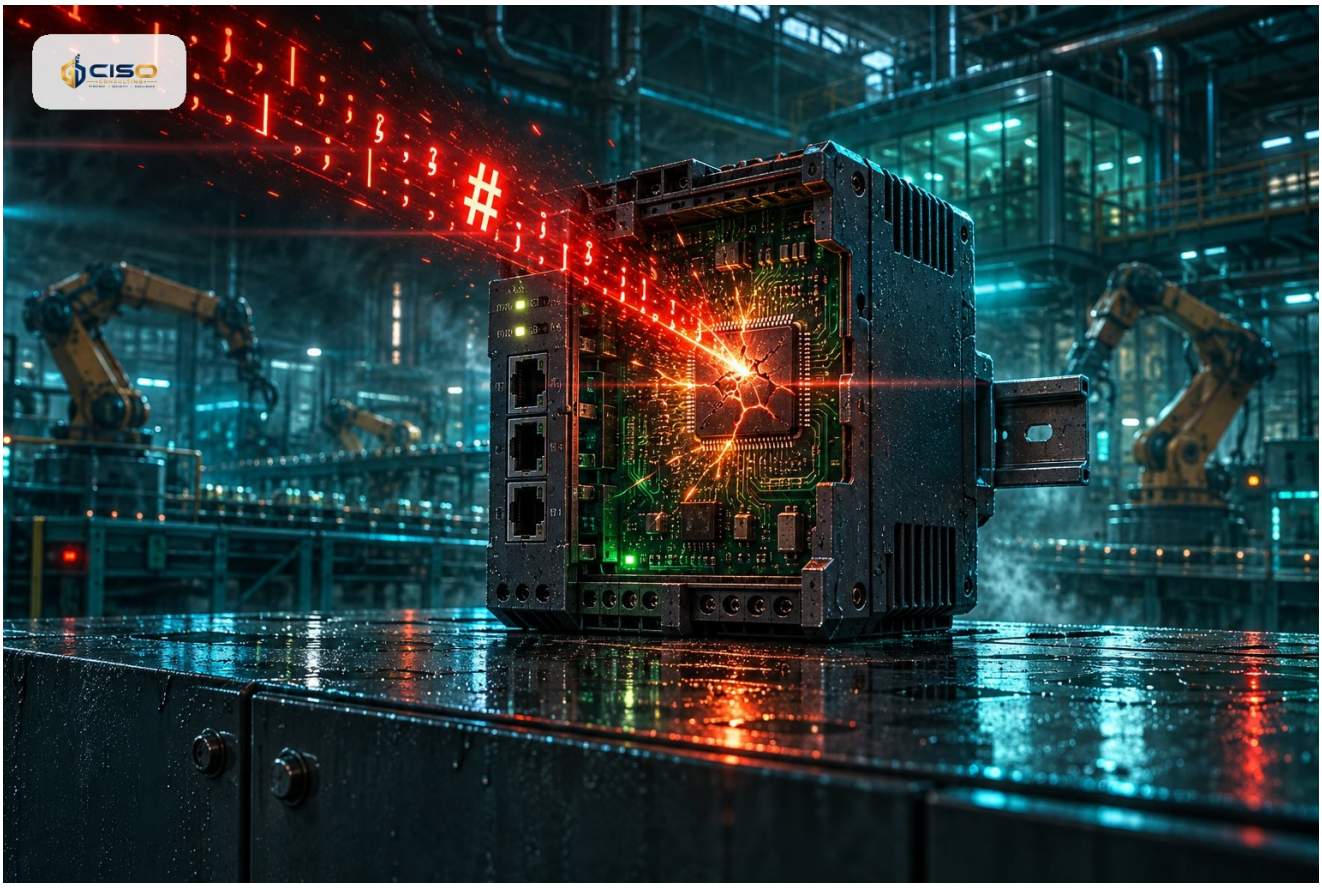
ثغرة في أداة تحديث البرنامج الثابت لـ Siemens meta-iot2050 تتيح تنفيذ أوامر بصلاحيات الجذر (CVE-2026-109830)



أصدرت CISA تنبيهًا عن ثغرة حقن أوامر (CVE-2026-109830، CVSS v3 بدرجة 7.3) في أداة تحديث البرنامج الثابت لـ meta-iot2050 بدءًا من V01.03.01. وتعمل Siemens على إصلاحات وتوصي بإجراءات تخفيف مؤقتة.

- المنتج المتأثر: Siemens meta-iot2050 بدءًا من الإصدار V01.03.01.
- الثغرة CVE-2026-109830 حقن أوامر نظام التشغيل في أداة تحديث البرنامج الثابت، بتقييم CVSS v3 قدره 7.3.
- من يستطيع تعديل ملف الإعدادات قد ينفّذ أوامر اعتباطية بصلاحيات الجذر.
- تنفّذ الأداة أجزاءً من ملف الإعدادات دون التحقق منها.

- تعمل Siemens على إصلاحات، ولا يوجد إصلاح متاح حاليًا بحسب التنبيه، لذا يُعتمد على إجراءات التخفيف.

نشرت CISA تنبيهًا خاصًا بأنظمة التحكم الصناعي عن ثغرة في Siemens meta-iot2050، وهو المشروع الذي تقوم عليه برمجيات أجهزة IOT2050 من الشركة. وتشمل الثغرة الإصدارات بدءًا من V01.03.01.

طبيعة الثغرة

تأخذ أداة تحديث البرنامج الثابت أجزاءً من ملف الإعدادات وتنفّذها دون التحقق منها. وهي ثغرة حقن أوامر في نظام التشغيل، معرّفة بالرقم **CVE-2026-109830** وبتقييم 7.3 وفق CVSS v3. وإذا تمكّن مهاجم من التلاعب بملف الإعدادات فقد يتمكن من تشغيل أوامر اعتباطية بصلاحيات الجذر على الجهاز.

ويذكر التنبيه قطاعات التصنيع الحيوي والطاقة وتقنية المعلومات، مع انتشار الأجهزة حول العالم. ومقر Siemens في ألمانيا.

الوضع الحالي

حالة المنتج «متأثر معروف»، ولا يُظهر التنبيه إصلاحًا متاحًا حاليًا. وتعمل Siemens على إعداد إصلاحات، وتوصي بإجراءات تخفيف للمنتجات التي لم تتوفر لها إصلاحات بعد.

يعتمد الاستغلال على قدرة المهاجم على تعديل ملف الإعدادات، لذا فإن ضبط من يملك صلاحية الكتابة عليه خطوة عملية أولى. وينبغي للجهات في المملكة التي تشغّل هذه الأجهزة في بيئات تشغيلية أو طرفية أن تتأكد من استخدامها، وتحدد الإصدارات، وتتابع إرشادات Siemens عند تحديثها.

ما يجب فعله الآن

1. حصر الأجهزة التي تعمل بـ meta-iot2050 بالإصدار V01.03.01 أو أحدث، بما فيها بيئات التقنية التشغيلية والطرفية.
2. حصر صلاحية الكتابة على ملف الإعدادات الذي تستخدمه أداة تحديث البرنامج الثابت في أقل عدد من مسؤولي النظام المصرح لهم.
3. تطبيق إجراءات التخفيف الواردة في تنبيه Siemens حيث لا يتوفر إصلاح، ومتابعة صدور الإصدار المصحَّح.
4. مراقبة ملفات الإعدادات ونشاط أداة التحديث لرصد أي تغييرات غير متوقعة أو أوامر تُنفَّذ بصلاحيات الجذر.
5. تسجيل التعرض في سجل مخاطر التقنية التشغيلية ومواءمة المعالجة مع متطلبات ضوابط الأمن السيبراني للأنظمة التشغيلية (NCA OTCC) والضوابط الأساسية (NCA ECC) لإدارة الثغرات.