CISA تحذّر من ثغرات حرجة في EPICS Base الإصدار 7.0.10 وما قبله



نشرت CISA إشعارًا بشأن EPICS Base الإصدار 7.0.10 وما قبله، وتبلغ درجة CVSS v3 للثغرات 9.8، وقد تتيح تعطيل الخدمة أو إتلاف الذاكرة أو تسريب المعلومات أو تنفيذ تعليمات برمجية.

- المتأثر: EPICS Base الإصدار 7.0.10 وما قبله.
- أربع ثغرات مدرجة: CVE-2026-114595 وCVE-2026-114596 وCVE-2026-114597 وCVE-2026-114598.
- درجة CVSS v3 تبلغ 9.8، وتشمل أنواع الضعف تجاوز الأعداد الصحيحة وعدم اتساق معامل الطول وتشويش الأنواع.
- الأثر المحتمل: تعطيل الخدمة وإتلاف الذاكرة وتسريب المعلومات وربما تنفيذ تعليمات برمجية عشوائية.
- يذكر الإشعار قطاع التصنيع الحيوي مع انتشار عالمي.

أصدرت CISA إشعارًا يخص أنظمة التحكم الصناعي بشأن EPICS Base من The EPICS Community، وأدرجت الإصدار 7.0.10 والإصدارات الأقدم ضمن النسخ المعروف تأثرها.

ما الذي يذكره الإشعار

يسرد الإشعار أربع ثغرات: CVE-2026-114595 وCVE-2026-114596 وCVE-2026-114597 وCVE-2026-114598.
وتندرج في ثلاثة أنواع من الضعف: **تجاوز الأعداد الصحيحة**، وعدم اتساق معامل الطول، و**تشويش الأنواع (Type Confusion)**. وتبلغ درجة CVSS v3 المسجلة 9.8.

وبخصوص CVE-2026-114595، يوضح الإشعار أن تجاوزًا في الأعداد الصحيحة عند معالجة طلبات الشبكة قد يؤدي إلى حجز ذاكرة بحجم غير صحيح، وقد تؤدي معالجة بيانات يرسلها المهاجم لاحقًا إلى إتلاف الذاكرة أو تعطيل الخدمة أو ربما تنفيذ تعليمات برمجية عن بُعد.

وبوجه عام قد يتيح الاستغلال الناجح تعطيل الخدمة أو إتلاف الذاكرة أو تسريب معلومات حساسة أو ربما تنفيذ تعليمات عشوائية. وتذكر CISA قطاع التصنيع الحيوي، مع انتشار المنتج عالميًا.

الخطوات المقترحة

لا يتضمن المقتطف الذي اطلعنا عليه تفاصيل خطوات المعالجة من المورّد، لذا ينبغي الرجوع إلى إشعار CISA الكامل وإرشادات المورّد. وعلى الجهات التي تشغّل EPICS Base في بيئات صناعية أو بحثية أن تحدد أولاً هل توجد نسخة بإصدار 7.0.10 أو أقدم، ثم تخطط للمعالجة وفق المعلومات المنشورة.

ما يجب فعله الآن

1. حصر جميع تثبيتات EPICS Base وتحديد أي نسخة بإصدار 7.0.10 أو أقدم.
2. مراجعة إشعار CISA الكامل وإرشادات المورّد لمعرفة خطوات المعالجة والتخفيف.
3. التخطيط للتحديثات أو إجراءات التخفيف واختبارها عبر إدارة التغيير قبل تطبيقها في الإنتاج.
4. الحد من تعرّض الأنظمة المتأثرة للشبكة وقصر الوصول إليها على الأجهزة المطلوبة فقط.
5. رصد الأنظمة المتأثرة بحثًا عن أعطال أو طلبات شبكة غير معتادة وتوثيق النتائج ضمن إجراءات الحوادث.