برنامج AutomationDirect C-More EA9: ثغرة تجاوز سعة الذاكرة تُستغل عبر ملفات مشاريع خبيثة



أصدرت CISA تنبيهاً عن الثغرة CVE-2026-127280 في برنامج C-More EA9 حتى الإصدار V6.80، إذ قد يؤدي ملف مشروع مُعدّ خصيصاً إلى تلف الذاكرة وتنفيذ شيفرة. درجة CVSS v3 هي 7.8.

- الإصدارات المتأثرة: برنامج C-More EA9 حتى الإصدار V6.80.
- الثغرة CVE-2026-127280 من نوع تجاوز سعة الذاكرة في الكومة (heap) بدرجة CVSS v3 تبلغ 7.8.
- لا يتحقق البرنامج بشكل كافٍ من البيانات المقروءة من ملف المشروع قبل استخدامها في عمليات ذاكرة الكومة.
- يتطلب الاستغلال أن يفتح المستخدم ملف مشروع خبيثاً قد يصل عبر البريد أو مشاركة الملفات أو وسائط التخزين القابلة للإزالة.
- يتراوح الأثر بين عدم استقرار التطبيق أو تعطله وإمكانية تنفيذ شيفرة تعسفية.

نشرت CISA تنبيهاً خاصاً بأنظمة التحكم الصناعي حول ثغرة في برنامج C-More EA9 Programming Software من AutomationDirect، تؤثر في الإصدار V6.80 وما قبله. تحمل الثغرة المعرّف CVE-2026-127280 ودرجة CVSS v3 تبلغ 7.8.

طبيعة الثغرة

لا يتحقق البرنامج بصورة كافية من البيانات التي يقرؤها من ملف المشروع قبل استخدامها في عمليات ذاكرة الكومة. وقد يتسبب ملف مُعدّ خصيصاً في تجاوز سعة الذاكرة عند فتحه، فيتلف جزء من الذاكرة ويضطرب عمل التطبيق. وتشير CISA إلى أن ذلك قد يؤدي إلى تعطل التطبيق، وربما إلى تنفيذ شيفرة تعسفية.

يعتمد الاستغلال على تفاعل المستخدم، إذ يجب إقناعه بفتح ملف مشروع خبيث. وتذكر النشرة وسائل التوصيل الشائعة مثل البريد الإلكتروني ومشاركة الملفات ووسائط التخزين القابلة للإزالة.

أهمية الأمر

تصنّف CISA القطاعات المعنية بالمنتج ضمن التصنيع الحرج والطاقة وأنظمة المياه والصرف الصحي، مع انتشار عالمي. وعلى الجهات في المملكة التي تشغّل تقنيات تشغيلية في هذه المجالات، أو تستخدم محطات هندسية تضم هذه الأداة، التحقق من وجودها في بيئتها.

لا يتضمن المقتطف الذي راجعناه إصلاحاً من الشركة المصنّعة أو إجراءات تخفيف محددة، لذا ينبغي الرجوع إلى نشرة CISA الكاملة والشركة المصنّعة للحصول على إرشادات المعالجة.

النهج المقترح

لأن الهجوم يتطلب فتح ملف، فإن ضبط طريقة وصول ملفات المشاريع إلى المحطات الهندسية يمثل خط الدفاع العملي الأول، إلى جانب التحقق من الإصدارات واتباع إرشادات الشركة المصنّعة.

ما يجب فعله الآن

1. حصر المحطات الهندسية وتحديد أي منها يستخدم C-More EA9 Programming Software بإصدار V6.80 أو أقدم.
2. مراجعة نشرة CISA الكاملة والتواصل مع AutomationDirect للحصول على إرشادات الإصلاح أو التخفيف.
3. عدم فتح ملفات المشاريع إلا من مصادر موثوقة ومتحقق منها، والتعامل بحذر مع الملفات غير المتوقعة الواردة عبر البريد أو مشاركة الملفات.
4. تقييد وسائط التخزين القابلة للإزالة المستخدمة في المحطات الهندسية وفحصها.
5. تنبيه مهندسي التقنيات التشغيلية والمقاولين القائمين على الصيانة إلى هذا الخطر المرتبط بالملفات.