CISA تحذّر من ثغرة تجاوز سفلي للأعداد الصحيحة في مكتبة libumqtt دون وجود إصلاح



أصدرت CISA تنبيهًا بشأن ثغرة تجاوز سفلي (CVE-2026-125132) في libumqtt حتى الإصدار 1.1.1 بتقييم CVSS v3 قدره 8.6، دون إصلاح متاح ودون استجابة من المطورين.

- تؤثر الثغرة CVE-2026-125132 في إصدارات libumqtt حتى 1.1.1 ضمنًا.
- قد يتمكن مهاجم عن بُعد من التسبب في حجب الخدمة أو إتلاف الذاكرة أو الكشف عن معلومات.
- درجة CVSS v3 تبلغ 8.6، ونوع الضعف CWE-191 (تجاوز سفلي للأعداد الصحيحة).
- لا يوجد إصلاح وفق CISA، ولم يستجب مالكو المستودع لطلب التنسيق.
- تذكر CISA قطاعات الاستخدام ومنها الطاقة والمياه والتصنيع وتقنية المعلومات والنقل.

نشرت CISA تنبيهًا خاصًا بأنظمة التحكم الصناعي بشأن libumqtt، وهي مكتبة تنفّذ بروتوكول MQTT. ويتناول التنبيه الثغرة CVE-2026-125132، وهي تجاوز سفلي للأعداد الصحيحة يؤثر في الإصدارات حتى 1.1.1 ضمنًا.

ما ورد في التنبيه

وفق CISA، قد يتمكن مهاجم عن بُعد من استغلال الثغرة للتسبب في حجب الخدمة أو إتلاف الذاكرة أو الكشف عن معلومات. وتصنَّف الثغرة ضمن CWE-191 وتبلغ درجتها 8.6 وفق CVSS v3.

وتذكر CISA أن القطاعات المعنية تشمل التصنيع الحرج والطاقة وتقنية المعلومات وأنظمة النقل والمياه والصرف، مع انتشار عالمي. وتُذكر الصين مقرًا للشركة.

لا يوجد إصلاح حتى الآن

ينص التنبيه على عدم توفر أي معالجة. ولم يستجب مالكو المستودع لطلب التنسيق من CISA، وتُشجَّع الجهات المستخدمة على التواصل مع المشروع عبر صفحته على GitHub.

الأثر العملي

لأن libumqtt مكتبة برمجية، فقد تكون مدمجة في أجهزة أو بوابات أو برمجيات داخلية دون أن تظهر في سجل التطبيقات المعتاد. لذا ينبغي أولاً التحقق من استخدامها، ثم الحد من انكشاف أي خدمات MQTT مبنية عليها إلى حين صدور إصلاح من المطورين أو من مورّد المنتج.

ما يجب فعله الآن

1. البحث في سجلات الأصول وقوائم SBOM وبرمجيات الأجهزة عن libumqtt بإصدار 1.1.1 أو أقدم.
2. مراسلة موردي أنظمة OT وإنترنت الأشياء للتأكد من تضمين المكتبة في منتجاتهم وطلب موقفهم من المعالجة.
3. حصر الوصول الشبكي إلى خدمات MQTT المتأثرة في شرائح موثوقة ومنع انكشافها على الإنترنت.
4. رصد الخدمات المتأثرة بحثًا عن أعطال أو إعادة تشغيل أو حركة MQTT غير معتادة.
5. تسجيل المخاطرة والضوابط البديلة في سجل المخاطر إلى حين توفر إصلاح أو بديل.