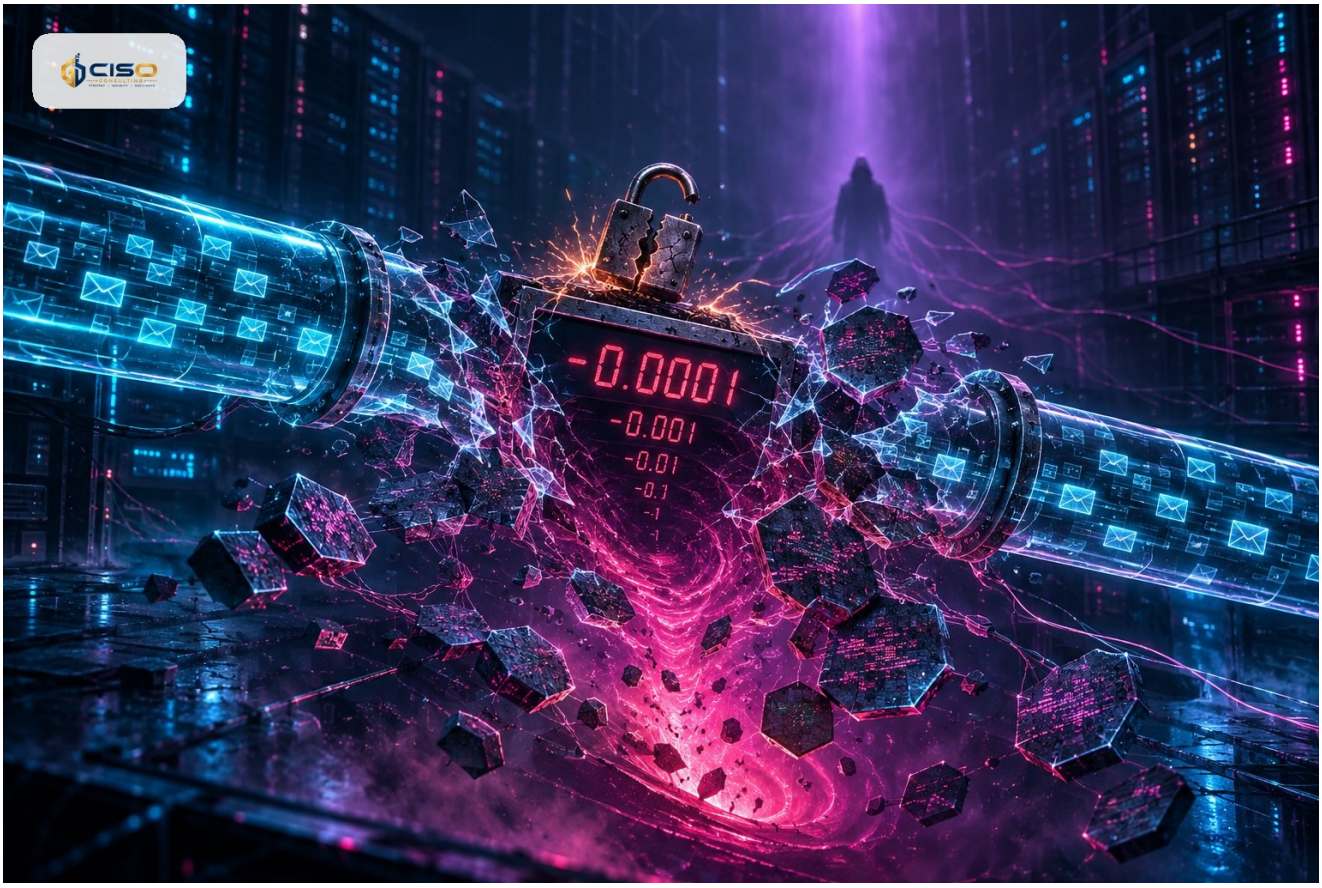
CISA تحذّر من ثغرة التفاف عددي في مكتبة libumqtt ولا يتوفر إصلاح



أصدرت CISA تنبيهًا عن ثغرة (CVE-2026-125132) في libumqtt الإصدار 1.1.1 وما قبله، قد تتيح لمهاجم عن بُعد تعطيل الخدمة أو إتلاف الذاكرة أو كشف المعلومات. لا يتوفر إصلاح.

- المتأثر: libumqtt الإصدار 1.1.1 وما قبله.
- الثغرة CVE-2026-125132 التفاف عددي (CWE-191) بدرجة CVSS v3 تبلغ 8.6.
- قد يتسبب مهاجم عن بُعد في تعطيل الخدمة أو إتلاف الذاكرة أو كشف المعلومات.
- لا يتوفر إصلاح، ولم يستجب مالكو المستودع لطلب التنسيق من CISA.
- تذكر CISA قطاعات منها الطاقة والمياه والتصنيع والنقل وتقنية المعلومات.

نشرت CISA تنبيهًا يخص أنظمة التحكم الصناعي بشأن مكتبة libumqtt، والإصدارات المتأثرة هي 1.1.1 وما قبله.

الثغرة المعرّفة بالرمز CVE-2026-125132 هي التفاف عددي (Integer Underflow) ويُعرف أيضًا بـ Wraparound، وتصنَّف ضمن CWE-191.

ما يذكره التنبيه

وفق CISA، قد يتمكن مهاجم عن بُعد يستغل الثغرة من تعطيل الخدمة أو إتلاف الذاكرة أو كشف معلومات. وتبلغ درجة CVSS v3 ما قيمته 8.6. ويورد التنبيه قطاعات منها التصنيع الحيوي والطاقة وتقنية المعلومات وأنظمة النقل والمياه والصرف الصحي، مع انتشار عالمي، ويذكر أن مقر الشركة في الصين.

لا يوجد إصلاح حتى الآن

تفيد CISA بأنه لا يتوفر أي إصلاح. ولم يستجب مالكو المستودع لطلب التنسيق، وتُشجَّع الجهات المستخدمة على التواصل مع المشروع عبر صفحته على GitHub للحصول على الدعم. ولا يذكر التنبيه حلاً بديلاً ولا يؤكد وجود استغلال فعلي للثغرة.

ماذا يعني ذلك لجهتكم

قد تكون المكتبة مضمَّنة في أجهزة أو تطبيقات وليست منتجًا مستقلاً، لذا فإن الخطوة الأولى هي معرفة ما إذا كانت موجودة لديكم. وعلى الجهات التي تشغّل معدات متصلة أو تبني برمجيات بمكونات مفتوحة المصدر مراجعة قوائم الأصول ومعلومات الموردين، ثم تطبيق ضوابط تعويضية ما دام الإصلاح غير متاح.

ما يجب فعله الآن

1. ابحثوا في قوائم الأصول البرمجية وSBOM وإفادات الموردين عن libumqtt بالإصدار 1.1.1 أو أقدم.
2. اسألوا موردي الأجهزة والتطبيقات المتصلة عن تضمينهم للمكتبة وخطتهم للمعالجة.
3. قيّدوا تعرّض خدمات MQTT المتأثرة للشبكة بحصرها في شرائح موثوقة وتحديد الوصول عن بُعد.
4. راقبوا الخدمات المتأثرة لرصد الانهيارات أو إعادة التشغيل أو الحركة غير المعتادة وسجّلوها للمراجعة.
5. وثّقوا التعرض في سجل المخاطر وتابعوا المشروع الأصلي لمعرفة صدور إصلاح.
6. فكّروا في استبدال المكتبة ببديل مدعوم حيث تُستخدم في برمجياتكم.