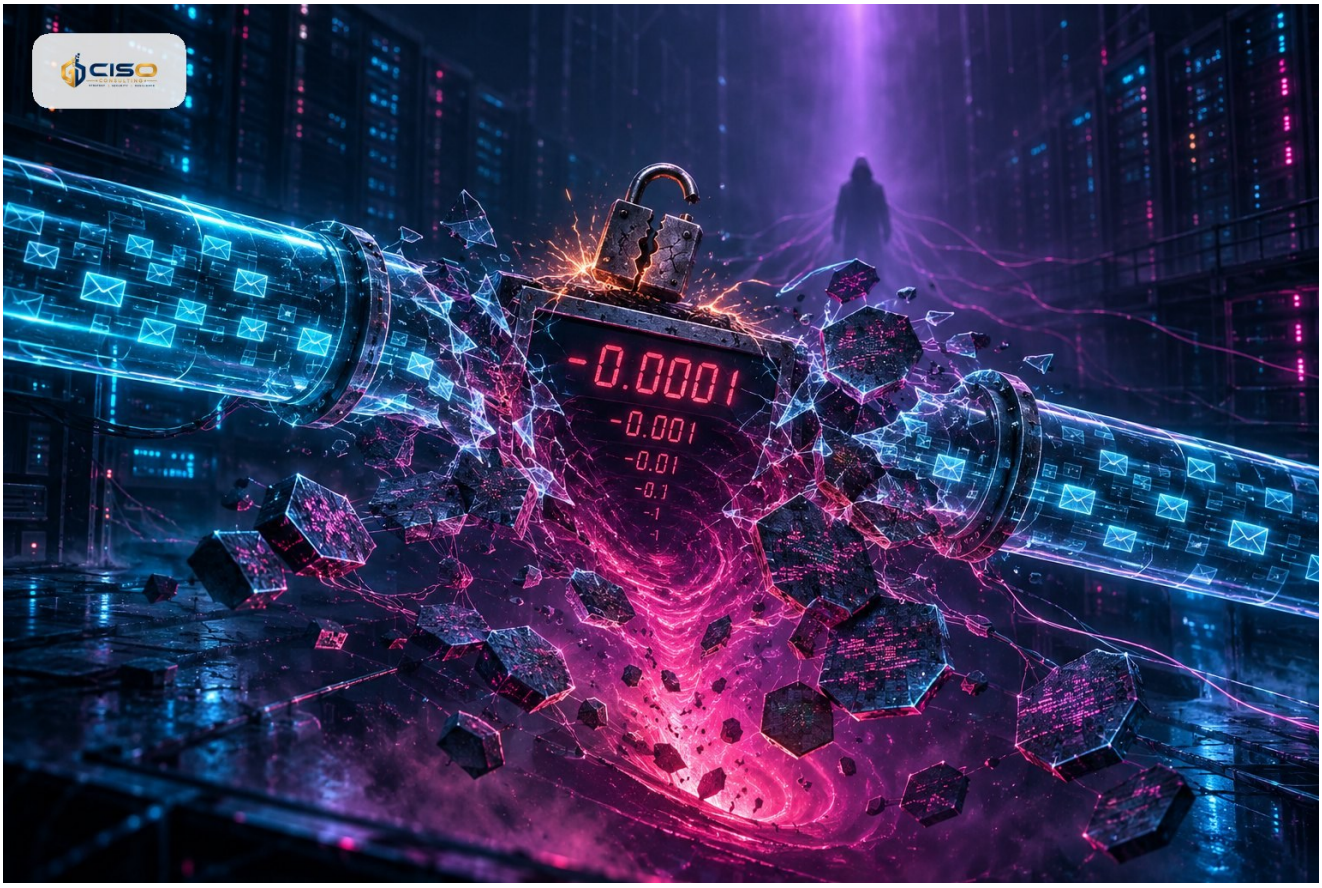
CISA flags integer underflow in libumqtt MQTT library; no fix available



CISA reports an integer underflow (CVE-2026-125132) in libumqtt 1.1.1 and earlier that a remote attacker could use for denial of service, memory corruption or information disclosure. No remediation is available.

- Affected: libumqtt version 1.1.1 and earlier.
- CVE-2026-125132 is an integer underflow (CWE-191) with a CVSS v3 score of 8.6.
- A remote attacker could cause denial of service, memory corruption or information disclosure.
- No remediation is available; the repository owners did not respond to CISA's coordination request.
- CISA lists sectors including energy, water, manufacturing, transportation and IT.

CISA has published an industrial control systems advisory on libumqtt, a library whose affected versions are 1.1.1 and earlier. The issue, tracked as CVE-2026-125132, is an integer underflow, also described as wrap or wraparound (CWE-191).

What the advisory says

According to CISA, a remote attacker who exploits the flaw could cause a denial of service, memory corruption or information disclosure. The CVSS v3 score is 8.6. The advisory lists critical manufacturing, energy, information technology, transportation systems, and water and wastewater among the relevant sectors, with worldwide deployment. The company is listed as headquartered in China.

No fix yet

CISA states that no remediation is available. The repository owners did not respond to its request for coordination, and users are encouraged to contact the project through its GitHub page for support. The advisory does not describe any workaround or confirm exploitation in the wild.

What this means for you

Because libumqtt may be embedded in devices or applications rather than installed as a standalone product, the first task is knowing whether it is present. Institutions that operate connected equipment or build software with open-source components should check their inventories and supplier information, then apply compensating controls while no patch exists.

What to do now

1. Search software inventories, SBOMs and supplier statements for libumqtt version 1.1.1 or earlier.
2. Ask vendors of connected devices and applications whether they embed libumqtt and what their mitigation plan is.
3. Restrict network exposure of any affected MQTT-based services to trusted segments and limit remote access.
4. Monitor affected services for crashes, restarts or unusual traffic, and log them for review.
5. Record the exposure in the risk register and track the upstream project for a fix.
6. Consider replacing the library with a maintained alternative where it is used in your own code.