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, rated CVSS v3 8.6. No remediation exists and the maintainers did not respond to coordination.

- CVE-2026-125132 affects libumqtt versions up to and including 1.1.1.
- A remote attacker could cause denial of service, memory corruption or information disclosure.
- CVSS v3 score is 8.6; the weakness is CWE-191, integer underflow.
- CISA lists no remediation, and the repository owners did not respond to its coordination request.
- CISA lists deployment in sectors including energy, water, manufacturing, IT and transportation.

CISA has published an industrial control systems advisory on libumqtt, a library implementing the MQTT

protocol. The advisory covers CVE-2026-125132, an integer underflow affecting versions up to and including 1.1.1.

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 issue is classified as CWE-191 (integer underflow, or wraparound) and carries a CVSS v3 score of 8.6.

CISA lists the affected sectors as critical manufacturing, energy, information technology, transportation systems, and water and wastewater, with worldwide deployment. The company is listed as headquartered in China.

No fix yet

The advisory states that no remediation is available. The repository owners did not respond to CISA's request for coordination, and users are encouraged to contact the project directly through its GitHub page.

Practical implications

Because libumqtt is a library, it may be embedded in devices, gateways or in-house software without appearing in a standard application inventory. Organisations should first establish whether they use it at all, then limit exposure of any MQTT services built on it until the maintainers or a vendor provide a fix.

What to do now

1. Search software inventories, SBOMs and device firmware for libumqtt version 1.1.1 or earlier.
2. Ask OT and IoT vendors whether their products embed libumqtt and request their mitigation position.
3. Restrict network access to affected MQTT services to trusted segments and block internet exposure.
4. Monitor affected services for crashes, restarts or abnormal MQTT traffic.
5. Record the risk and compensating controls in the risk register until a fix or replacement is available.