Denial of Service via Reachable Assertion in `PUBLISH` Packet Parsing

Moderate **HJianBo** published **GHSA-r3fr-7m74-q7g2** 3 weeks ago

Package

CocoaMQTT (Swift)

Affected versions	Patched versions
<2.2.2	2.2.2

Description

A vulnerability exists in the packet parsing logic of CocoaMQTT that allows an attacker (or a compromised/malicious MQTT broker) to remotely crash the host iOS/macOS/tvOS application.

The vulnerability is located in `Source/FramePublish.swift` during the extraction of the Topic string from the incoming byte array.

When parsing the Variable Header of a `PUBLISH` frame, the library reads the first two bytes to determine the `topicLength`. It then adds this length to the current position (`pos`) and attempts to slice the byte array to extract the string:

```
if let data = NSString(bytes: [UInt8](bytes[2...(pos-1)]), length: Int(len), encoding:
    topic = data as String
}
```

If a packet is received where the Topic Length evaluates to `0` (e.g., `0x00 0x00`), the `len` variable becomes `0`, and `pos` evaluates to `2`.

The slicing logic dynamically calculates `bytes[2...(2-1)]`, which becomes **`bytes[2...1]`**. Swift's `ClosedRange` operator (`...`) requires the lower bound to be less than or equal to the upper bound. Because 2 is not less than 1, Swift detects an out-of-bounds access attempt and immediately triggers a runtime trap (`Fatal error: Range requires lowerBound <= upperBound`), crashing the host application.

If an attacker publishes this 4-byte malformed payload to a shared topic with the `RETAIN` flag set to true, the MQTT broker will persist the payload. Any time a vulnerable client connects and subscribes to that topic, the broker will automatically push the malformed packet. The app will instantly crash in the background before the user can even interact with it. This effectively "bricks" the mobile application (a persistent DoS) until the retained message is manually wiped from the broker database.

Severity

Moderate 5.7 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H

CVE ID

CVE-2026-30867

Weaknesses

▶ CWE-617

Credits

 **t5uki** Reporter