

Vulnerability Overview

Cesanta Mongoose

MQTT Integer Overflow Vulnerability (CVE-2019-19307)

Vulnerability Rating

Critical

CVSS v3 9.8



Introduction

Cesanta Mongoose is a lightweight embedded networking library that includes an MQTT broker implementation. CyStack identified a critical vulnerability in the MQTT packet parsing logic that can be exploited remotely over the network, without authentication, when an affected MQTT service is exposed.

Synopsis

CVE-2019-19307 is an **integer overflow vulnerability** in the function `parse_mqtt` (in `mongoose.c`) affecting Cesanta Mongoose 6.16.

A remote attacker can send a crafted MQTT packet to trigger denial of service (infinite loop) and may be able to reach out-of-bounds memory access conditions (with potential for further impact depending on usage and compilation/runtime context).

Details

MQTT uses a variable-length "Remaining Length" field (1–4 bytes). Mongoose decodes this field in a loop and accumulates the decoded value into `len`. In the affected code path, a crafted sequence can cause integer overflow/wraparound during the length calculation. This can make the computed packet "end" pointer become smaller than expected, enabling:

- **Remote DoS by preventing the broker from consuming/removing the crafted message** from the input buffer, resulting in an infinite processing loop.
- **Potential out-of-bounds access (read/write)** if downstream logic uses the corrupted length/end calculations unsafely.

Timeline

- **October 2, 2019:** CyStack reported the issue to the Cesanta Mongoose team.
- **October 18, 2019:** CyStack requested a CVE from MITRE.
- **November 26, 2019:** CVE-2019-19307 assigned/published.
- **February 11, 2020:** Maintainer indicated the fix was released in Mongoose 6.17.

Learn more

[CyStack Advisories](#)

[NIST Vulnerability Database](#)