MQTT CVE Security Report

2025-08-13 11:43:46

Broker Information

- **IP Address:** 192.168.15.211
- **Port:** 1883
- **Version:** mosquitto version 2.0.16
- **CPE:** cpe:2.3:a:eclipse:mosquitto:2.0.16:*:*:*:*:*:*:*

Executive Summary

This report summarizes known vulnerabilities affecting the Mosquitto MQTT broker.
Total CVEs found: 3
• Critical (9.0–10.0): 1
• High (7.0–8.9): 1
• Medium (4.0–6.9): 1
• Low (0.1–3.9): 0
• Unscored / Unknown: 0

Critical (9.0–10.0) (1 CVEs)

CVE ID: CVE-2024-10525
CVSS Score: 9.8
Published: 2024-10-30T12:15:02
Summary: In Eclipse Mosquitto, from version 1.3.2 through 2.0.18, if a malicious broker sends a crafted SUBACK packet with no reason codes, a client using libmosquitto may make out of bounds memory access when acting in its on_subscribe callback. This affects the mosquitto_sub and mosquitto_rr clients.
References:

- https://github.com/eclipse-mosquitto/mosquitto/commit/8ab20b4ba4204fdcdec78cb4d9f03c944a6e0e1c
- https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/190
- https://mosquitto.org/blog/2024/10/version-2-0-19-released/

High (7.0–8.9) (1 CVEs)

CVE ID: CVE-2024-8376
CVSS Score: 7.5
Published: 2024-10-11T16:15:14
Summary: In Eclipse Mosquitto up to version 2.0.18a, an attacker can achieve memory leaking, segmentation fault or heap-use-after-free by sending specific sequences of "CONNECT", "DISCONNECT", "SUBSCRIBE", "UNSUBSCRIBE" and "PUBLISH" packets.
References:

- https://github.com/eclipse-mosquitto/mosquitto/commit/1914b3ee2a18102d0a94cbdbbfeae1afa03edd17
- https://github.com/eclipse/mosquitto/releases/tag/v2.0.19
- https://gitlab.eclipse.org/security/cve-assignement/-/issues/26
- https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/216
- https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/217
- https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/218
- https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/227
- https://mosquitto.org/

Medium (4.0–6.9) (1 CVEs)

CVE ID: CVE-2024-3935
CVSS Score: 6.5
Published: 2024-10-30T12:15:03
Summary: In Eclipse Mosquito, versions from 2.0.0 through 2.0.18, if a Mosquitto broker is configured to create an outgoing bridge connection, and that bridge connection has an incoming topic configured that makes use of topic remapping, then if the remote connection sends a crafted PUBLISH packet to the broker a double free will occur with a subsequent crash of the broker.
References:

- https://github.com/eclipse-mosquitto/mosquitto/commit/ae7a804dadac8f2aaedb24336df8496a9680fda9
- https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/197
- https://mosquitto.org/blog/2024/10/version-2-0-19-released/

Additional Tests

The following test modules were run, and here are their results:

Error reading file auth-check.json: Extra data: line 2 column 1 (char 93)
Test: fingerprint-matched
Result: "fingerprint": "Mosquitto2122 1.3.1-1.3.5"