MQTT to CAN gateways are not affected

Trend Micro Research reported security vulnerabilities in respect to MQTT and CoAP. Providers of CAN/MQTT gateways answered to us that their products are not affected.

CAN/MQTT gateways should be used in secure environments (Photo: Adobe Stock)

Message Queuing Telemetry Transport (MQTT) is a communication protocol used in both IoT (Internet of Things) and IIoT (Industrial Internet of Things) applications. MQTT is a publisher-subscriber protocol that facilitates one-to-many communication mediated by brokers. Clients can publish messages to a broker and/or subscribe to a broker to receive certain messages. Messages are organized by topics, which essentially are “labels” that act as a system for dispatching messages to subscribers.

The Constrained Application Protocol (CoAP) is a client-server protocol that, unlike MQTT, is not yet standardized. With CoAP, a client node can command another node by sending a CoAP packet. The CoAP server interprets it, extracts the payload, and decides what to do depending on its logic. The server does not necessarily has to acknowledge the request.

MQTT is preferred over CoAP for mission-critical communications because it can enforce quality of service and ensure message delivery. CoAP, for its part, is preferred for gathering telemetry data transmitted from transient, low-power nodes like tiny field sensors.

Trend Micro Research outlined design issues and implementation vulnerabilities, which can contribute to the number of unsecure deployments. A design issue that the researchers discovered (designated as CVE-2017-7653 for Mosquitto, the most popular broker), for instance, can allow a malicious client to supply invalid data. By using the message-retain option and modifying the quality of service (QoS), an attacker can lead clients to be flooded with the same (retained) message over and over. Unsecure endpoints, moreover, can expose records and leak information, some of which are related to critical sectors, for any casual attacker to see. Vulnerable endpoints can also run the risk of denial-of-service (DoS) attacks or even be taken advantage of to gain full control.

CAN Newsletter Online asked some providers of CAN/MQTT gateway, if their products were affected by the above-mentioned research results. SYS TEC (Germany) answered that their products use the possibility to run TLS communication, “This makes the complete communication path secure against cyber-attacks,” explained Klaus Rupprecht from SYS TEC. “MQTT follows a simple rule: Make the things easy and not complex, due to this fact you’ll have the overview and 100-percent ownership about the system.”

Andreas Boebel from Emtas (Germany) responded: “Despite being very active in the standardization of CANopen, CANopen FD, and related IIoT activities our CANopen-MQTT gateway implementation was not released as a product yet. We will look into the current security issues with MQTT and reschedule our CANopen-MQTT plans accordingly after a thorough evaluation of the security risks. No release date is planned yet. Our existing CiA 309-2 and CiA 309-3 gateway solutions are not affected by the MQTT security issues.”

HMS’ offers CAN products from its Ixxat business unit, which evaluated the mentioned vulnerabilities, too. Christian Schlegel, head of the HMS Technology Center Ravensburg (Germany), stated that the CAN@net NT gateway is not affected by the mentioned security issue due to several design-features. To avoid DoS (denial of service) situations as well as disruption of the connection between the device and the broker, the CAN@net does only publish telegrams but does not have MQTT receive functions. This also helps to avoid issues due to a broker or client interrupting the connection, if an MQTT topic contains a not UTF-8-coded string: If the broker does not monitor this but the client does, the attacker is able to switch-off the client with just one message. Because the CAN@net just publishes messages and does not subscribe MQTT topics from the client, these attacks are not possible. Also, the CAN@net NT disables all networking ports that are not configured for operation to inhibit other ways of attacks. “We recommend to our customers that they should use their own local broker in an secure environment,” added Schlegel. “As MQTT is basically a very light-weight protocol with limited security elements, it is always risky to use a public broker, because attackers can read and might also manipulate data either by man-in-the middle attacks or by simply subscribing to data from the broker depending on safety settings of broker and data to be published.

hz