

Konformitätsbewertung

Im Rahmen einer Sicherheitsanalyse hat die

AWARE7 GmbH

am Standort

Munscheidstr. 14

45886 Gelsenkirchen

die Systemarchitektur sowie einen Datenauszug des Netzwerkverkehrs der **WAN-Verbindung via „TLS-over-LoRaWAN“** als Teilkomponente der IoT-Anwendung loTree®

hinsichtlich der korrekten Nutzung des DTLS (Datagram Transport Layer Security) -Protokolls und der analog angewandten Anforderungen der folgenden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten technischen Richtlinien für die Sicherheitsanforderungen an den Einsatz kryptographischer Verfahren bei der WAN-Kommunikation intelligenter Messsysteme:

„Kryptografische Vorgaben für Projekte der Bundesregierung, Teil 3 – intelligente Messsysteme“ insbesondere die Anforderungen aus Kapitel 4 und Kapitel 2 (BSI-TR-03116-3, Version vom 23. Februar 2022)

und

„Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS)“ (BSI TR-02102-2, Version vom 24.01.2022)

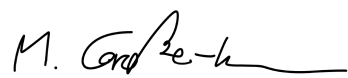
überprüft.

Die Überprüfung der Auswahl der kryptographischen Verfahren (kryptographische Basisverfahren, Domainparameter für Elliptische Kurven), des Umganges mit Ephemerschlüsseln und Lebensdauern sowie der sicheren Zufallszahlengenerierung stellten den Fokus der Analyse dar. Geprüft wurde der Gitlab Commit mit dem Hashwert "e2c18af26f0c64da82254ab250cb74a5f33fcf64".

Die Überprüfung erfolgte vom 10.10.2022 bis zum 14.10.2022 mit einem Zeitbudget von 7 Personentagen.

Im Rahmen dieses Tests und Umfang wurden keine Konformitätsverstöße gegen die Anforderungen der technischen Richtlinien festgestellt. Details zu den Ergebnissen der Sicherheitsanalyse sowie deren Rahmenbedingungen sind in dem Prüfbericht Prüfbericht-Physec_V2_2022-10-17 aufgeführt.

Gelsenkirchen, 17.10.2022



Dr. Matteo Große-Kampmann
Geschäftsführung