Honeywell

THE POWER OF **CONNECTED**

Technische Information zu den Flow Computern der enCore-Serie

Elster Honeywell produziert und vertreibt elektronische Messeinrichtungen vom Typ enCore. Diese Messeinrichtungen werden typisch als Mengenumwerter (Baureihen ZM1, BM1, FC1), zur Stationsüberwachung und als Daten-Gateway (Baureihe MC1) eingesetzt.
Jedes enCore-Gerät kann mit bis zu drei LAN-Schnittstellen ausgestattet werden. Damit kann jedes enCore-Gerät in bis zu drei separaten IP-Netzwerken gleichzeitig kommunizieren.

Elster GmbH
Steinern Straße 19-21
55252 Mainz-Kastel
Deutschland

T +49 (0)6134 605-0
F +49 (0)6134-605-204
customerfirst@honeywell.com
www.elster.com

09.08.2019

Elster Honeywell bestätigt hiermit folgende Eigenschaft der LAN-Schnittstellen und der zugehörigen in den enCore-Messeinrichtungen hinterlegten Programmierung („IP-Stack"):

- In den Messeinrichtungen sind keine Mechanismen enthalten, die es ermöglichen, zwischen den unterschiedlichen Netzwerken zu kommunizieren und dabei die Messeinrichtung als Router zu verwenden.
- Es ist somit nicht möglich, über eines der Netzwerke Information zur Struktur und Topologie der anderen Netzwerke zu ermitteln oder mit Teilnehmern in den anderen Netzwerken zu kommunizieren.
- Diese Eigenschaft wurde durch Expertise (Penetrationstest) eines unabhängigen Unternehmens für IT-Sicherheit untersucht und im Rahmen eines Testberichts bestätigt.

Detailinformation

In der oben genannten Expertise wurden folgende Punkte an den LAN-Schnittstellen der enCore Messeinrichtungen überprüft.

1. Allgemein
    - Aufdecken von verwendeter Software und deren Versionen
    - Recherche bezüglich verwendeter Software- und Hardwarekomponenten bezüglich Schwachstellen und öffentlicher Exploits
2. Netzwerk
    - Portscan zum Aufdecken offener Ports an den Netzwerkschnittstellen
    - Unterschiede in statischer Adressvergabe und DHCP der jeweiligen Netzwerkschnittstellen
    - Simulation von Netzwerk-Anomalien zum Detektieren von Fehlverhalten aufgrund von Abweichungen im Netzwerk
    - Aufbau diverser Netzwerktopologien zum Testen des Ausbruchs in das andere Netzwerk (Netzwerk-Hopping)
    - Simulation von Spanning Tree Protokoll Anfragen, um Fehlverhalten festzustellen
    - Netzwerkstabilitätsprüfung während des Boot-Vorgangs

Honeywell
THE POWER OF CONNECTED

3. Protokoll-Applikationsschicht
    - Webserver Tests (nach OWASP TOP10)
    - Webserver Protokoll Fuzzing
    - Modbus TCP Protokoll Fuzzing
    - Veränderung und gezielte Abänderung der Konfigurationsanfragen über die MMS Schnittstelle
    - Ansatz eines MMS Protokoll Fuzzings auf Grundlage der durch die enSuite Applikation entstandene Kommunikation zur Konfiguration und Statusabfrage des Flow Computers
    - Automatisierte Scans auf alle Protokolle

Mit freundliche Grüßen,

Christian Neugebauer
Technology Manager Gas Electronics

Marcin Klekot
Team leader Embedded Software