HMS Security Advisory Report

HMSSAR-2019-05-29-001
Publication date: 29 May 2019

Ewon Security Enhancement (Fixed in 13.1s0)

Ewon reference: Webserver - Ewon authentication mechanism improvement

**Affected devices:** All

**Affected firmware versions:** From 12.2 to 13.0

**Status:** Fixed

**Severity:** Low (CVSS 3 Score of 3.7)

**Description:**
A non-authenticated user could get access in read only to some Ewon device information. This is not impacting Talk2M users, only the Ewon local users are concerned.

**Mitigation Factors:**
As a rule, we recommend:

- to avoid making Ewons devices being directly reachable from non-trusted user by using a firewall and an access control policy.
- use a secure remote access solution like Talk2M.

**Solution:**
Install the last firmware version. This has been fixed as from version 13.1s0.
Discovered by: Tijl Deneut - Howest (UGent) and Hodei López & Ander Martínez, members of the company Titanium Industrial Security, participants in a project linked to the National Network of Industrial Laboratories (RNLI) of the National Institute of Cybersecurity (INCIBE).