HMS Security Advisory Report

HMSSAR-2019-06-16-001

Publication date: 20 June 2019
Last update: 02 July 2019

Overview

An independent researcher and a PEN-testing company have discovered and disclosed a vulnerability linked to a configuration parameters encryption weakness (including the device local users' password). Their finding shows that the encryption of these parameters is weak due to an implementation issue in the encryption mechanism function.

Note that to perform this attack, the potential attacker needs to get access to the device local configuration file, meaning that he must be connected to the device with an admin account.

Impact

Successful exploitation of this vulnerability may allow a remote attacker to get access to the local system and perform potential harmful actions on the device itself, but also on devices connected to the Ewon device.

Affected products and versions

- Ewon Flexy & Cosy 131 device families – Prior to firmware version 13.3
- Ewon Cosy 141 and CD device families – Prior to firmware version 11.3

Severity / CVSS Score

The CVSS [1]severity base score is 6.8, and the associated scoring vector is
CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

[Use https://www.first.org/cvss/calculator/3.0]

https://www.first.org/cvss/cvss-v30-user_guide_v1.5.pdf

HMS Recommendations

HMS recommends that the products is updated to latest firmware version (>= 13.3 for the Ewon Flexy & Cosy 131 families and >= 11.3 for the Ewon Cosy 141 and CD families) where the issue has been fixed.

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 (https://www.ewon.biz/cloud-services/talk2m).

Product updates

An update that completely fixes the problem is available here:
https://websupport.ewon.biz/support/product/manual-firmware-update/manual-firmware-download

[1] CVSS is owned by FIRST and used by permission. https://www.first.org/cvss

Acknowledgements

HMS thanks Tijl Deneut from Howest (UGent) and Stu Kennedy from PentestPartners for finding and notifying about the vulnerability in a controlled way.

Additional information

Ewon website vulnerability notification: https://websupport.ewon.biz/support/news/support/ewon-security-vulnerability