HMS Security Advisory Report

HMSSAR-2020-02-07-001

Publication date: 07 February 2020
Last update: 20 May 2020 (Updated CVSS Link)

Overview
An independent researcher has discovered a cross-site scripting vulnerability.

Impact
If successful, an attacker could trigger a password change performing a CSRF attack or compromise the administrator machine using some browser exploit. XSS Victim must introduce credentials before code is executed.

Affected products and versions
- Flexy and Cosy products – Prior to firmware version 14.1s0

Severity / CVSS Score

https://www.first.org/cvss/user-guide

HMS Recommendations
HMS recommends that the products is updated to latest firmware version (from 14.1s0) where the issue has been fixed.

Product updates
An update that completely fixes the problem is available here: https://ewon.biz/technical-support/pages/all-downloads.

Acknowledgements
HMS thanks Ander Martínez from Titanium Industrial Security for finding and notifying about the vulnerability in a controlled way.

Additional information
Ewon website vulnerability notification: https://www.hms-networks.com/cybersecurity

---

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