Vulnerability Report – CubeOne

Description

An unauthenticated attacker with access to the local network is able to obtain a copy of the diagnostic logs from the CubeOne device.

Platform

The following devices and versions have been used during the test:

- CubeOne:
  - Firmware Version - 2.2.4.10

Impact

CVSS v3 Severity and Metrics:

- Base Score: 4.3
- Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
- Impact Score: 1.4
- Exploitability Score: 2.8

Steps to reproduce

The vulnerability requires the attacker to have access to the local network on which the device resides.

The attacker is able to obtain a copy of the diagnostics logs from the CubeOne device without authentication needed.

The logs contain sensible information such as the interaction the user had with the cube one or the sensor logs. Other sensible information could be present but has not been studied.

A proof of concept script is provided (ismartalarm.py), the script can be used to obtain the diagnostic logs from the device. Some example data can be parsed using the script.

Refer to the README included as well as the command line help (-h) for information about dependencies and usage of the script.

Recommendations

The diagnostic logs can contain sensible data, the endpoint to collect them should be authenticated, and the traffic should be encrypted.

Francesco Servida
University of Lausanne
In collaboration with Seculabs SA