Overview
On December 9th 2021, a 0-day exploit in the Java logging library log4j (version 2) published as CVE-2021-44228, (critical CVSSv3 10) was divulged. This vulnerability has been completed by CVE-2021-45046. This vulnerability has been completed by CVE-2021-45105. This vulnerability has been completed by CVE-2021-44832.

Impact
Remote Code Execution (RCE) by logging a certain string.

Affected Apache log4j2 versions
2.0 ≤ Apache log4j ≤ 2.14.1 for CVE-2021-44228
2.0 ≤ Apache log4j ≤ 2.15 for CVE-2021-45046
2.0 ≤ Apache log4j ≤ 2.16 for CVE-2021-45105
2.0 ≤ Apache log4j ≤ 2.17 for CVE-2021-44832

Ewon statement CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832
HMS/Ewon has made the necessary patching on his Talk2M (including M2Web) cloud infrastructure. Cosy, Flexy and Ewon CD devices are not concerned by the vulnerability.

HMS/Ewon highly recommends updating the eCatcher Windows software to its latest version (eCatcher 6.7.9, including version 2.17.1 of log4j at publication date of this report) to prevent exploitation of this vulnerability (see release note history).
eCatcher Mobile applications (IOS and Android) are not concerned by the vulnerability.
viewON application is not concerned by the vulnerability.
All Netbiter Hardware including EC, WS, and LC devices are not concerned by the vulnerability.

Product updates
Product updates are available here: https://www.ewon.biz/technical-support/pages/all-downloads.

HMS Recommendations
Monitor HMS Security Advisory page which is updated as soon as new information is available about Security.

Additional information