Kramer's response to CVE-2021-44228 Apache Log4j

Background

CVE-2021-44228 is a remote code execution vulnerability discovered on December 9, 2021. It directly affects Apache Log4j, which is widely used for open-source Java logging purposes for client and server applications.

Investigation Summary

Kramer completed a thorough analysis of its products and determined that two products were affected by the Log 4j vulnerability, with resolutions as noted:

1. **KronoMeet Cloud** – A software release that resolves the Apache Log4j vulnerability can be downloaded as follows:
    - From the Kramer KronoMeet product page – Please download the KronoMeet Android Application Version 1.0.1221.100.
    - KronoMeet Cloud using KramerAppUpdate on the KronoMeet Device.
    - Google Play – Kramer VIA application (For KT107-SC users).

   For more details, please refer to the KronoMeet Release Notes.

2. **VIA Android Application** – A software update that resolves the Apache Log4j vulnerability can be downloaded as follows:
    - From the Kramer VIA product page – Please download the VIA Android Application Version 3.2.1221.490.

   For more details, please refer to the VIA Release Notes.

No other Kramer products are affected by the Apache Log4j vulnerability.