CYBERSECURITY VULNERABILITY ADVISORY

Log4j - Vulnerability

Document: CYB/2021/44463/Advisory
Revision: 1.1
Date: 22-DECEMBER-2021

External Vulnerability ID(s):

CVE ID: CVE-2021-44228

DISCLAIMER

The information in this document is subject to change without notice and should not be construed as a commitment by Kalkitech / ASE.

Kalkitech/ASE provide no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Kalkitech, ASE or any of their suppliers be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if Kalkitech/ASE have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from Kalkitech/ASE and the contents hereof must not be provided to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Summary

This advisory relates to the recently announced Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228).

Log4j is NOT included or used in any ASE products including ASE2000, ASE61850, ASEDLMS, SPT-PC, SpTsrv, SAM or Bell 202 Modems. Further Log4j is NOT included or used in Kalkitech SYNC family of products including SYNC 200, 2000, 2100, 3000, 4000 series. These products are not Java based applications and do not use any Java components and therefore are not impacted by this vulnerability

Further, CVE-2021-44228 does not impact Kalkitech's kalki.io middleware, both Cloud version and On-Premise version and Eltrix which does not use the impacted library.