December 16, 2021

Re: Log4Shell Vulnerability in Log4j. No effect on i3 customers.

To all our customers and partners;

On December 9, 2021 a zero-day arbitrary code execution vulnerability in a popular Java logging framework Log4j has been publicly disclosed by the Alibaba Cloud's security team and was given the descriptor Log4Shell (CVE-2021-44228). This vulnerability was said to have existed unnoticed since 2013. Apache Software Foundation, the company in charge of Log4j project, has assigned Log4Shell a CVSS (Common Vulnerability Scoring System) rating of 10 (highest severity).

Effect on i3 customers

None of the i3 software or hardware products are affected by this vulnerability. No action is required by i3 product users.

What is Log4j and how does Log4Shell vulnerability work?

Log4Shell vulnerability takes advantage of Log4j's allowing requests to arbitrary LDAP and JNDI servers, allowing attackers to execute arbitrary Java code on a server or other computer, or leak sensitive information. A list of its affected software projects has been published by the Apache Security Team. Affected commercial services include many enterprise cloud environments.

References:

https://en.wikipedia.org/wiki/Log4Shell
https://logging.apache.org/log4j/2.x/security.html
https://blogs.apache.org/security/entry/cve-2021-44228
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/

Please contact technical support if you have any questions or issues

i3 International Technical Support and Services
Email: support@i3international.com
Tel.: 1.877.877.7241

CONTACT US
www.i3international.com
Toll free: 1.866.840.0004
Tel: 416.261.2266
Fax: 416.759.7776

CANADA
i3 International Inc.
780 Birchmount Rd, Unit 16
Toronto, Ontario
M1K 5H4, Canada

USA
i3 America (Nevada) Inc.
4001 Cobb International Boulevard,
Kennesaw, GA 30152