27 December 2021

Dear Customers,

Nihon Kohden Corporation

Response to Log4 Shell Vulnerability

1. Analysis of the vulnerabilities

Nihon Kohden continues our analysis of the remote code execution vulnerabilities related to Apache Log4j (a logging tool used in many Java-based applications) disclosed on 9 Dec 2021. Currently, Nihon Kohden is not aware of any impact to its modality as a result of this vulnerability.

As we continue our investigation, **we will notify our customers via our global website if we identify any impact to our products.**

To help customers protect themselves, we are also providing the following information to help customers improve their security posture.

2. As a general guideline Nihon Kohden recommends all customers maintain good security posture and isolation of NK equipment from other devices

１） Please make sure that the equipment connected to the network is secured by blocking the hospital network from the external network, such as a firewall.

２） Please make sure that no unauthorized equipment is connected to the network in the hospital.

3. Background of Log4j

The vulnerabilities, tracked as CVE-2021-44228 and CVE-2021-45046 and referred to as "Log4Shell," affects Java-based applications that use Log4j 2 versions 2.0 through 2.15.0. Log4j 2 is a Java-based logging library that is widely used in business system development, included in various open-source libraries, and directly embedded in major software applications. The scope of impact has expanded to thousands of products and devices, including Apache products such as Struts 2, Solr, Druid, Flink, Swift, Karaf, and others.

Because these vulnerabilities are in a Java library, the cross-platform nature of Java means the vulnerabilities are exploitable on many platforms, including Windows, macOS, and Linux. As many Java-based applications can leverage Log4j 2 directly or indirectly, organizations should contact application vendors or ensure their Java applications are running the latest up-to-date version. Developers using Log4j 2 should ensure that they are incorporating the latest version of Log4j into their applications as soon as possible to protect users and organizations.

Detail information

More information is available from CISA Apache Log4j Vulnerability Guidance.
https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
Official Note from CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-45046
Vender Release Note:
https://logging.apache.org/log4j/2.x/

*1 Java: A programming language that can operate platform-independent

4. Contact Us

Please feel free contact our following URL with any questions and concerns.
Contact Us | Nihon Kohden Global Site