Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

2021 Hanwha Techwin S-Cert Team

12/15/2021, updated 12/23/2021

Log4j Vulnerability Report

■ OVERVIEW

✓ The Log4j vulnerability was published on December 10, 2021, as CVE-2021-44228 (Known as Log4Shell).

✓ **CVE-2021-44228**

The vulnerability affects Apache **2.0-beta9 <= Log4j <=2.14.1** JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

■ RESULTS

✓ **The following Hanwha Techwin products (Network Camera, NVR/DVR/Pentabrid Recorder, WAVE VMS, SSM VMS, etc.,) DO NOT utilize or embed Log4j. Therefore, there is no effect on our products and no action needs to be taken.** **(Not Vulnerable)**

✓ The OSSA Android-based cameras (ONO-9081R, ONV-9081R) have been confirmed by Azena (OS provider) that the Operating System is not affected by the Log4j vulnerability. **(Not Vulnerable) (Updated 12/23/2021)**

✓ The Wisenet SKY Cloud VMS does use the Log4j software, which was vulnerable. The Apache software foundation released a patch to fix the vulnerability on December 11, 2021. The patch has been deployed. No action needs to be taken by the customer or dealer. **(Not Vulnerable, remediated)**

✓ Log4net is used for SSM, but the log4j vulnerability is not affected by Log4net.

➢ The Apache Logging Services Project creates and maintains open-source logging frameworks for public use. These services are listed below:

- **Apache Log4j: Logging framework for Java, JSP. (Vulnerable)**
- Apache Log4php: Logging framework for PHP. **(Not Vulnerable)**
- Apache Log4net: Logging framework for the Microsoft .NET. **(Not Vulnerable)**
- Apache Log4cxx: Logging framework for C++. **(Not Vulnerable)**

* If you have further questions regarding this vulnerability, please contact the Hanwha Techwin S-CERT team (secure.cctv@hanwha.com).