

2021 Hanwha Techwin S-Cert Team

12/15/2021

12/23/2021 (Updated)

## Log4j Vulnerability Report

### ■ OVERVIEW

- ✓ Log4j vulnerability has been found as CVE-2021-44228 (Known as Log4Shell).
- ✓ **CVE-2021-44228**

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, SSM VMS, WAVE VMS, etc.) DO NOT utilize or embed Log4j. Therefore, there is no effect on our products and no action needs to be taken.
- ✓ Regarding the OSSA Android-based camera (ONO-9081R, ONV-9081R), Hanwha is inquiring with the OS provider.
  - Azena (OS provider) has confirmed that their OS has not been affected by Log4j vulnerability. **(Not Vulnerable) (Updated, 12/23/2021)**
- ✓ Log4net is used for SSM, but this log4j vulnerability is not affected by Log4net.
  - The Apache Logging Services Project creates and maintains open-source logging frameworks to 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](mailto:secure.cctv@hanwha.com)).