Hanwha Vision

6, Pangyo-ro 319beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, Korea
TEL 82.70.7147.7000 FAX 82.31.8018.3702 www.HanwhaVision.com

2023 Hanwha Vision S-Cert Team

12/06/2023

SSM/MGM Ransomware Notice via Apache ActiveMQ Vulnerability (CVE-2023-46604)

■ OVERVIEW

- This vulnerability (CVE-2023-46604) is regarding Remote Code Execution without authentication using Java OpenWire protocol in Apache ActiveMQ.
- Hanwha Wisenet SSM/MGM have used Apache ActiveMQ v5.16.4 (vulnerable version) and need to be updated with v5.16.7 (non-vulnerable version).
- Risk of ransomware attack has been reported using this vulnerability.
  Refer: https://www.malwarebytes.com/blog/business/2023/11/apache-activemq-vulnerability-used-in-ransomware-attacks
- Hanwha has agreed with the need to provide advance notice to our customers with regard to this critical vulnerability.

■ AFFECTED PRODUCTS AND SOFTWARE

- This Apache ActiveMQ vulnerability CVE-2023-46604 affects **Hanwha Wisenet SSM software and related Appliances**.
  ※ This does not affect Hanwha's other cameras, storage devices or software except for the above products and software.
- Refer to the below table for the affected software and appliances, affected software version, and corrected software version.

Software / Appliance	Affected Software Version	Corrected Software Version
SSM / SSM Appliance	2.14.00 and prior versions	2.14.01 and later versions
MGS Appliance	1.01.02 and prior versions	1.01.03 and later versions

Hanwha Vision

6, Pangyo-ro 319beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, Korea
TEL 82.70.7147.7000 FAX 82.31.8018.3702 www.HanwhaVision.com

■ Risk Mitigation and Required Action

- Please do not use Internet via public network until the patched version is installed in your PC / Appliances.
- If a public network connection is unavoidable, we recommend using it with equipment that can detect/prevent intrusions, such as IDS/IPS.
- Please update the affected software and appliances with the patched version as soon as possible. Software can also be downloaded from Hanwha Vision websites.
- When installing the corrected software version, existing settings and video data are preserved as is when installing the existing SSM upgrade version, and separate backup/recovery procedures are not required.
- However, if infected with ransomware, recovery of existing settings and video data is impossible and the risk of additional infection is high, so full format (delete) and reinstallation are required.
- If you have any questions, please feel free to reach out the Hanwha S-CERT team at secure.cctv@hanwha.com or your local Technical Support Team.