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

2023/12/06

# Apache ActiveMQ の脆弱性を介したSSM/MGMランサムウェアの通知 (CVE-2023-46604)

## ■ 概要

- 本脆弱性(CVE-2023-46604)は、Apache ActiveMQでJava OpenWireプロトコルを使用した認証なしのリモートコード実行に関するものです。
- Hanwha Wisenet SSM/MGMは、Apache ActiveMQ v5.16.4 (脆弱性のあるバージョン)を使用しており、v5.16.7 (脆弱性のないバージョン)に更新する必要があります。
- 本脆弱性を使用したランサムウェア攻撃のリスクが報告されています。
  参照: https://www.malwarebytes.com/blog/business/2023/11/apache-activemq-vulnerability- used-in-ransomware-attacks
- Hanwhaは、この重大な脆弱性に関して顧客に事前の通知を行い、リスクを緩和できる方法を案内する必要があると判断しました。

## ■ 影響を受ける製品およびソフトウェア

- 本Apache ActiveMQの脆弱性( CVE-2023-46604)は、**Hanwha Wisenet SSM softwareおよび関連アプライアンス製品**に影響します。
  ※ 上記の製品およびソフトウェアを除くその他のHanwha製品（カメラ、ストレージデバイス、またはソフトウェア）には影響しません.
- 影響を受けるソフトウェアとアプライアンス製品、影響を受けるソフトウェアバージョン、および修正されたソフトウェアバージョンについては、以下の表を参照してください。.

| ソフトウェア/アプライアンス | 影響のあるソフトウェアバージョン | 修正されたソフトウェアバージョン |
|---|---|---|
| SSM / SSM Appliance | 2.14.00 及び以前のバージョン | 2.14.01 及び以降のバージョン |
| MGS Appliance | 1.01.02 及び以前のバージョン | 1.01.03 及び以降のバージョン |

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

## ■ リスク軽減方法及び必要な処置

- パッチを適用したバージョンがPC/アプライアンスにインストールされるまでは、パブリックネットワーク経由でインターネットを使用しないでください。
- パッチを適用したバージョンは、インターネットのパブリックネットワークが可能な別のPCから当社のホームページからダウンロードした後、USB経由でパブリックネットワークに接続できないお客様のPCおよびアプライアンスに再インストールしてください。
- パブリックネットワーク接続が避けられない場合は、IDS/IPSなどの侵入を検出または防止できる機器との併用を推奨します。
- 該当するソフトウェアおよびアプライアンス製品をできるだけ早くパッチが適用されたバージョンにアップデートしてください。ソフトウェアは、Hanwha Visionのウェブサイトからもダウンロードできます。
- 修正されたソフトウェアバージョンをインストールする場合、既存の設定と録画データは既存のSSMのバージョンアップを行った際と同様に保持されます。**個別のバックアップ/リカバリ手順は必要ありません。**
- 但し、ランサムウェアに感染した場合、既存の設定や録画データの復旧は不可能であり、追加感染のリスクが高いため、フルフォーマット(削除)と再インストールが必要となります。
- ご質問がございましたら、Hanwha S-CERTチームsecure.cctv@hanwha.comにお問い合わせください。