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 한화비전 S-CERT팀

12/07/2023

Apache ActiveMQ 취약점 (CVE-2023-46604)을 악용한 SSM 랜섬웨어 위험성 고지

■ 개요

- 본 취약점 (CVE-2023-46604)은 Apache ActiveMQ 내의 Java OpenWire 프로토콜을 사용하여 인증없이 원격으로 코드를 실행할 수 있는 취약점입니다.
- 한화 와이즈넷 SSM은 Apache ActiveMQ의 취약한 버전인 v5.16.4을 사용하고 있었으므로, 취약하지 않은 v5.16.7버전으로 업데이트가 필요합니다.
- 본 취약점을 악용한 랜섬웨어 공격의 위험성이 보고되고 있습니다.
  참고: https://www.malwarebytes.com/blog/business/2023/11/apache-activemq-vulnerability-used-in-ransomware-attacks
- 이에, 당사는 본 취약점의 심각성에 관하여 고객들에게 사전 고지하고 이러한 리스크를 완화할 수 있는 방안을 안내하는 것이 필요하다고 판단하였습니다.

■ 영향받는 모델 및 소프트웨어

- 본 Apache ActiveMQ 취약점인 CVE-2023-46604은 **한화 와이즈넷 SSM 소프트웨어 및 관련 어플라이언스 제품**에 영향을 주고 있습니다.
  ※ 본 취약점은 위에서 언급된 제품 및 소프트웨어를 제외한 한화의 카메라/저장장치 제품군 및 소프트웨어에는 영향을 주지 않습니다.
- 영향받는 소프트웨어와 관련 어플라이언스 제품, 영향받는 소프트웨어 버전, 개선된 소프트웨어 버전에 대한 정보는 아래 표를 참고해주시기 바랍니다.

소프트웨어 / 어플라이언스	영향받는 소프트웨어 버전	개선된 소프트웨어 버전
SSM / SSM 어플라이언스	2.14.00 및 이전버전	2.14.01 및 이후버전
MGS 어플라이언스	1.01.02 및 이전버전	1.01.03 및 이후버전

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

■ 리스크 완화 방안 및 필요 조치 사항

- 고객 PC 및 어플라이언스에 개선된 버전이 설치되기 전까지 인터넷 공용망을 통한 네트워크 연결을 하지 말아 주십시오.
- 개선된 버전은 인터넷 공용망이 가능한 또다른 PC를 통해 당사 홈페이지에서 다운로드 받으신 후 USB를 통해 공용망 접속이 불가한 고객 PC 및 어플라이언스에 재설치 해주시기 바랍니다.
- 공용망 접속이 불가피한 경우 IDS/IPS 같은 침입 탐지 시스템 또는 침입 방지 시스템 장비를 사용하여 외부 공격으로부터 안전하게 보호할 수 있는 방법으로 연결하시는 것을 추천드립니다.
- 사용하시는 제품 및 버전이 영향받는 대상이라면, 가능한한 빨리 개선된 버전을 당사 홈페이지에서 다운로드 받아 업데이트해주십시오.
- 개선된 버전 설치 시 기존의 SSM 업그레이드 버전 설치와 동일하게 기존의 설정 및 영상 데이터는 그대로 보존되며 별도의 백업/복구 절차는 필요 없습니다.
- 그러나, 이미 랜섬웨어에 감염된 경우에는 기존 설정 및 영상 데이터의 복구가 거의 불가능하고 추가적인 감염의 위험이 크므로 전체 포맷(삭제) 후 재설치가 필요합니다.
- 문의 사항이 있으신 경우 한화 S-CERT팀(secure.cctv@hanwha.com)이나 현지 기술지원팀으로 연락주시기 바랍니다.