Hanwha Techwin

White paper

안전한 SNMP 사용 가이드

2020 년 9 월 22 일

Contents

개정 이력

버전	개정일자	개정내용	비고
v1.0	20200922	최초 작성	

1. 서비스 거부 공격 사례 발생

최근 공용망에 직접 노출된 당사 카메라의 SNMP 서비스를 이용해 서비스 거부 공격을 수행한 사례가 발견되었습니다. 본 악용 사례는 공용망에 설치된 카메라에 해당하며, 내부망이나 로컬망에 설치된 카메라에는 해당하지 않습니다. 또한, 공용망에 연결이 되어 있다 하더라도 SNMP 서비스가 비활성화되어 있는 카메라들 역시 영향이 없습니다.

문제가 되는 해당 SNMP 서비스는 최신 버전 SNMP v3가 아닌, v1, v2c 버전에만 해당하며, 구버전(iPOLiS 포함, 2018년 이전 출시된 Wisenet 제품) 카메라 모델에서는 v2c 버전이 기본으로 활성화되어 있어서 해당 서비스를 사용할 의도가 없었더라도 서비스 거부 공격의 수단으로써 악용될 수 있으므로 주의해야 합니다.

이에 한화테크윈은 본 "안전한 SNMP 사용 가이드" 문서를 통해 제품에 구현된 SNMP 서비스의 보안 기능을 안전하게 사용할 수 있도록 안내하고자 합니다.

2.1. "SNMP 서비스" 소개

SNMP(Simple Network Management Protocol) 란, 간단한 네트워크 관리를 위한 규약으로, 네트워크 상 장비들의 모니터링, 환경설정 및 운영을 할 수 있도록 해주는 관리 프로토콜입니다. 네트워크 관리자는 SNMP를 통해 아래 내용들을 수행 할 수 있습니다.

네트워크 구성 관리

네트워크상 호스트들의 연결 구조를 파악하고 관리 할 수 있습니다.

성능 및 장비 관리

각 네트워크 세그먼트(Segment)간 네트워크 사용량, 에러량, 처리속도, 응답시간 등 성능 분석에 필요한 통계정보를 확인 할 수 있으며, 특정 장비의 시스템 정보(CPU, MEMORY, DISK 사용량)도 확인 할 수 있습니다.

보안 관리

정보의 제어 및 보호 기능이 있습니다. 특히, 가장 최신 버전인 SNMP v3는 정보보호를 위한 기능이 향상 되었습니다.

2.2. 공용망 연결 시 SNMP 서비스 안전하게 사용하기

SNMP 서비스는 관리 편의를 제공하지만 잘못된 사용 시, 서비스 거부 공격(DoS), 비인가 접속 등 문제점 발생의 원인이 되기도 합니다.

이에 한화테크윈의 최신 카메라 모델에는 서비스 거부 공격을 야기할 수 있는 SNMP 서비스가 초기 비활성화 되어 있으며, 필요에 따라 선택적으로 활성화 시킬 수 있도록 옵션을 제공하고 있습니다. 또한, SNMP 서비스를 안전하게 사용할 수 있도록 SNMP v3 버전을 제공하고 있습니다.

현재 사용하고 있는 카메라의 SNMP 서비스를 악용한 보안 사고를 예방하기 위해 다음의 사항이 적용되었는지 점검해 주시기 바랍니다.

2.2.1 최신 펌웨어 업데이트

SNMP 서비스 보안강화 설정을 지속 유지 하고, 향후 안전하게 관리하기 위해서는 최신 펌웨어로 업데이트를 해야합니다. 펌웨어 업데이트 후, 최신 보안설정 환경을 적용하기 위해 공장초기화 작업 또한 반드시 필요합니다

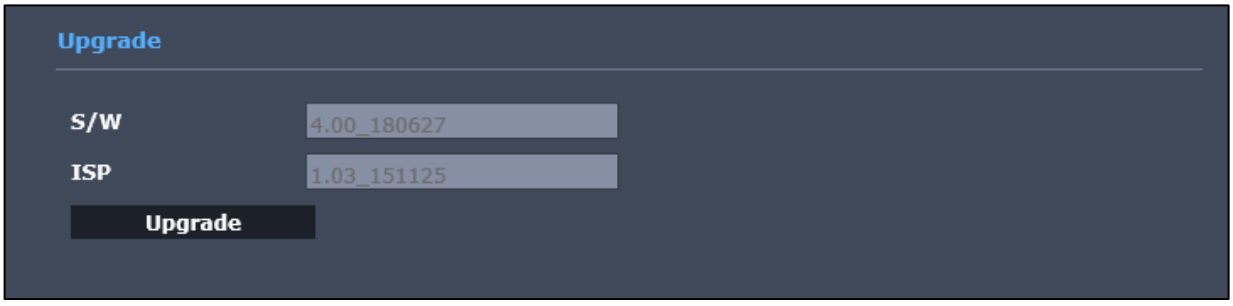
1) 한화테크윈 홈페이지(www.hanwha-security.com)에서 해당 모델명 검색 후, 최신 펌웨어 다운로드

2) 아래 메뉴를 통해 펌웨어 업그레이드 수행

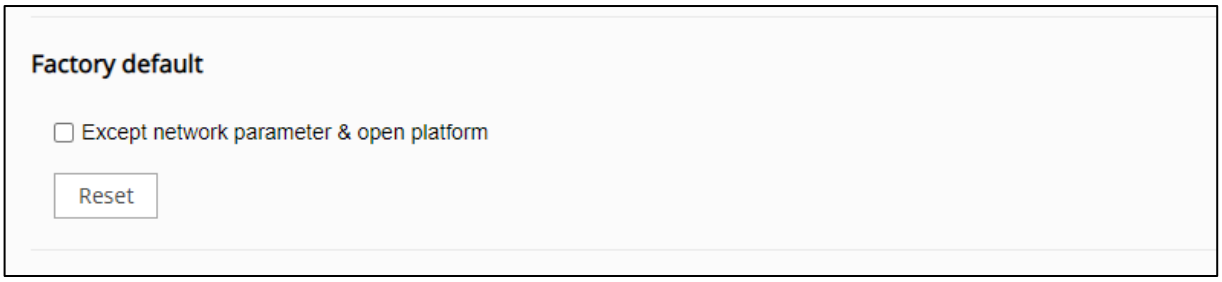
   메뉴: 설정 → 시스템 → 업그레이드

3) 업그레이드 완료 후, 공장 초기화 (네트워크 설정 유지 **해제**)

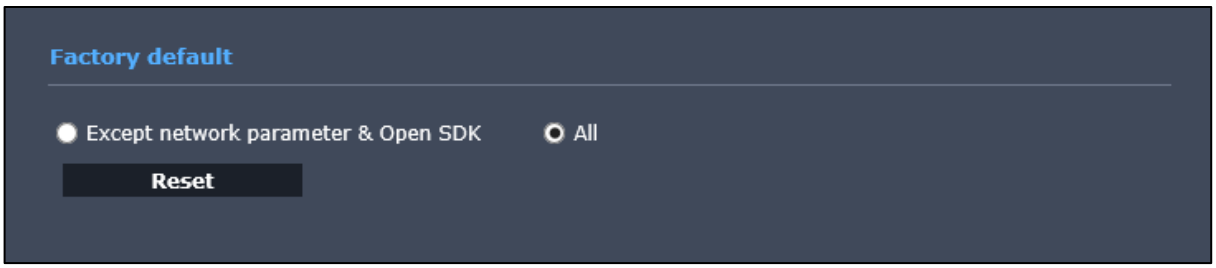
[펌웨어 업그레이드 기능]



[구버전 카메라의 펌웨어 업그레이드 기능]



[공장초기화 시 네트워크 설정 유지 체크 해제]



[구버전 카메라의 공장초기화 시 네트워크 설정 유지 체크 해제]

Q&A) 펌웨어 업그레이드 후, SNMP 설정 변경을 또 해야 하나요?

당사 장비는 펌웨어 업그레이드 이후에도 사용자 기존 설정을 그대로 유지하도록 되어 있습니다. 따라서 펌웨어 업그레이드 후, SNMP 설정까지 변경해야 안전한 보안설정을 할 수가 있습니다.

(참고: 2.2.2 SNMP 서비스 비활성화 적용)

Q&A) 공장초기화 시, "네트워크 설정 유지" 옵션은 무엇인가요?

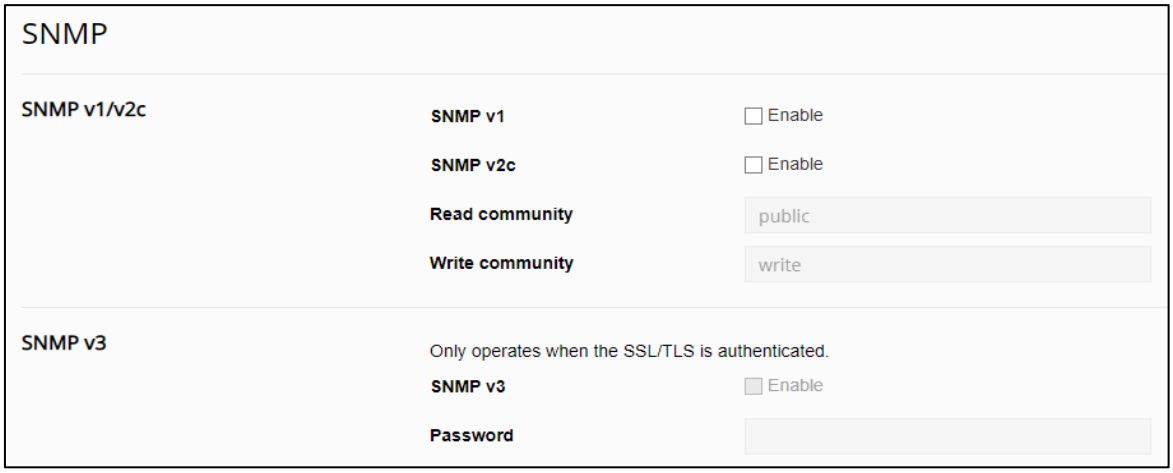
장비에 설정된 네트워크 관련 설정(IP, 프로토콜 모드, SNMP 설정 등)을 그대로 유지하면서 공장초기화를 수행하는 옵션입니다. "네트워크 설정 유지" 옵션을 선택 할 경우, 기존의 SNMP 설정이 유지되므로, 안전한 보안설정을 위해서는 "네트워크 설정 유지" 옵션을 해제한 후 초기화해야 합니다.

2.2.2 SNMP 서비스 비활성화 적용

SNMP 서비스를 사용하지 않는데 해당 기능이 활성화되어 있다면, 서비스 기능 설정에서 SNMP 서비스를 선택 해제해 기능을 제한할 수 있습니다.

1) 메뉴: 설정 → 네트워크 → SNMP

2) SNMP v1, v2c 및 v3 모두 선택 해제



[비활성화된 SNMP 서비스]

[구버전 카메라의 비활성화된 SNMP 서비스]

Q&A) SNMP 비활성화가 안되요

2017년 이전 펌웨어를 사용하는 장비는 SNMP 서비스 전체를 비활성화 할 수 없습니다. 이 경우 보유하고 계신 당사 장비의 최신 펌웨어를 한화테크윈 홈페이지(www.hanwha-security.com)에서 업데이트 한 뒤, 비활성화가 가능합니다.

2.2.3. SNMP v3 사용

네트워크 관리를 위해 SNMP 서비스가 필요할 경우, 안전한 SNMP v3 버전 사용을 권장합니다. SNMP v3은 네트워크를 통한 패킷 인증 및 암호화 기술을 조합하여 장치에 보안 접근(Access) 기능을 제공합니다. SNMP v3에서 제공되는 보안 기능은 다음과 같습니다.

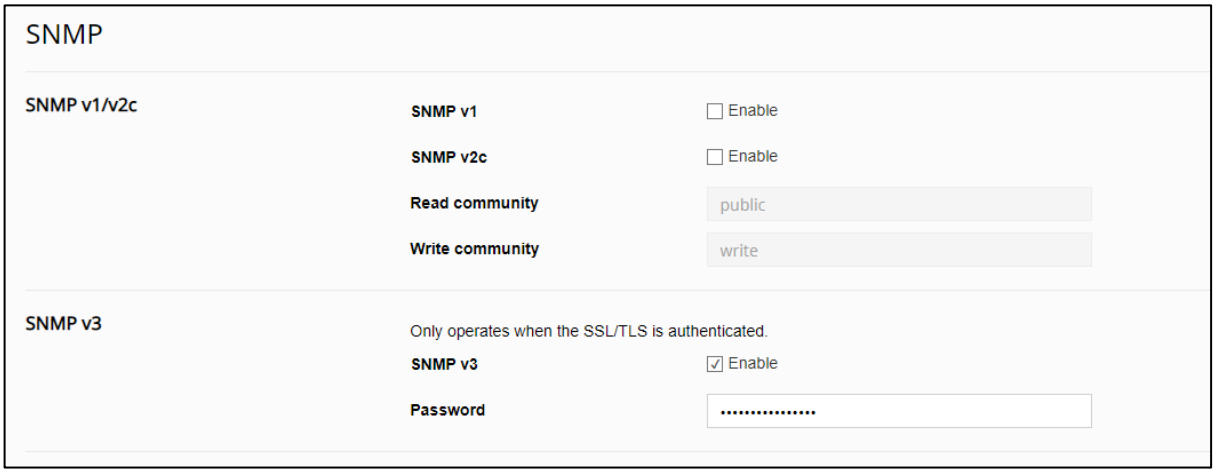
- 메시지 무결성 - 패킷이 전송 중에 조작되지 않도록 합니다.
- 인증 - 메시지의 출처가 유효한지 확인합니다.
- 암호화 - 권한이 없는 원본에서 패킷을 볼 수 없도록 패킷 콘텐츠를 암호화합니다.

SNMP v3 설정은 아래의 방법으로 설정할 수 있습니다.

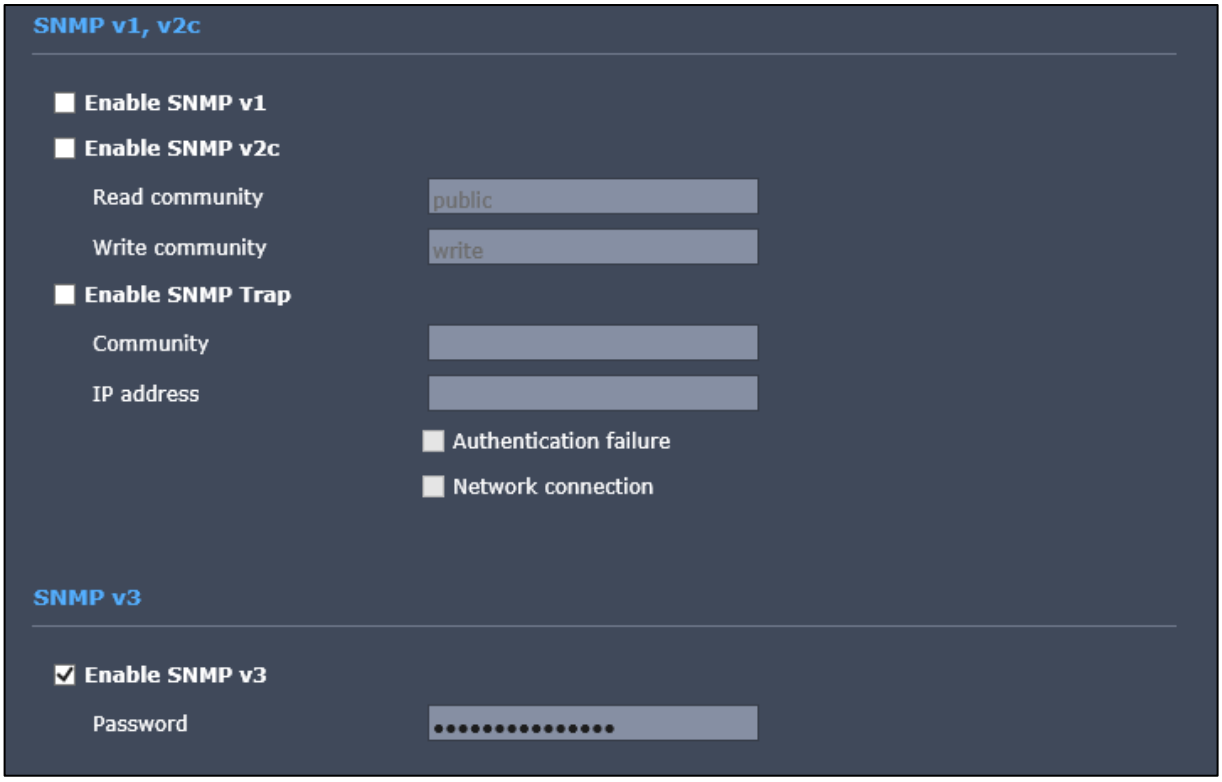
1) HTTPS 모드 설정 (메뉴: 설정 → 네트워크 → HTTPS 또는 SSL)

2) SNMP v3 활성화 및 비밀번호 설정 (메뉴: 설정 → 네트워크 → SNMP)

※ 비밀번호는 영문자, 숫자를 포함한 8자리 이상 구성을 권고



[활성화된 SNMP v3 서비스]



[구버전 카메라의 활성화된 SNMP v3 서비스]

2.2.4. SNMP Community String 변경

부득이하게 SNMP v1, SNMP v2c를 사용할 수 밖에 없는 경우, 인증을 위해 사용되는 SNMP 프로토콜의 초기 Community String을 “public” 대신 제 3자가 추측 할 수 없는 문자열 구성으로 변경해 적용하면 더욱 안전한 네트워크 관리 환경을 구축 할 수 있습니다.

예시) 8자 길이 이상의 영문자+숫자 조합 문자열: owa3fxpzmj

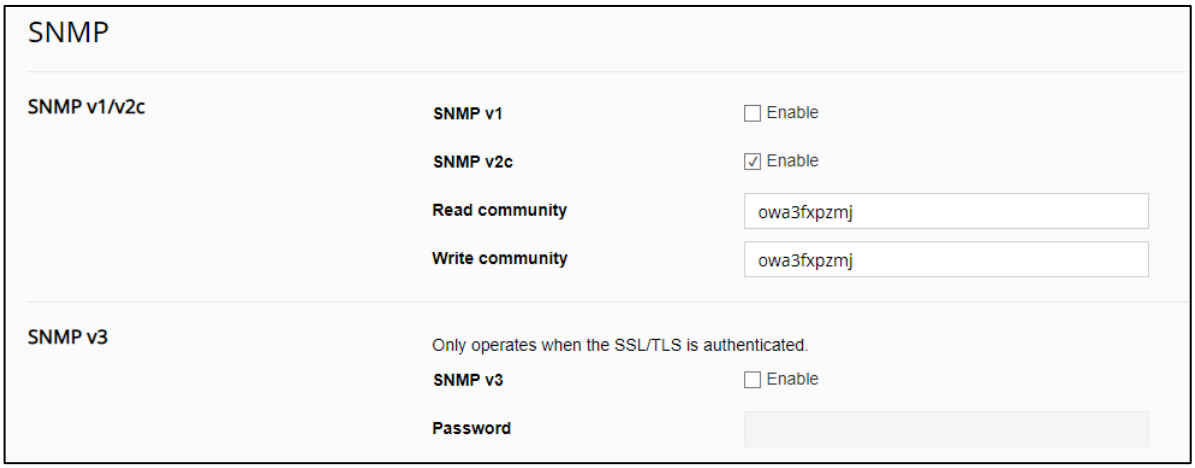
1) 메뉴: 설정 → 네트워크 → SNMP

2) Read Community String을 추측하기 어려운 문자열로 변경

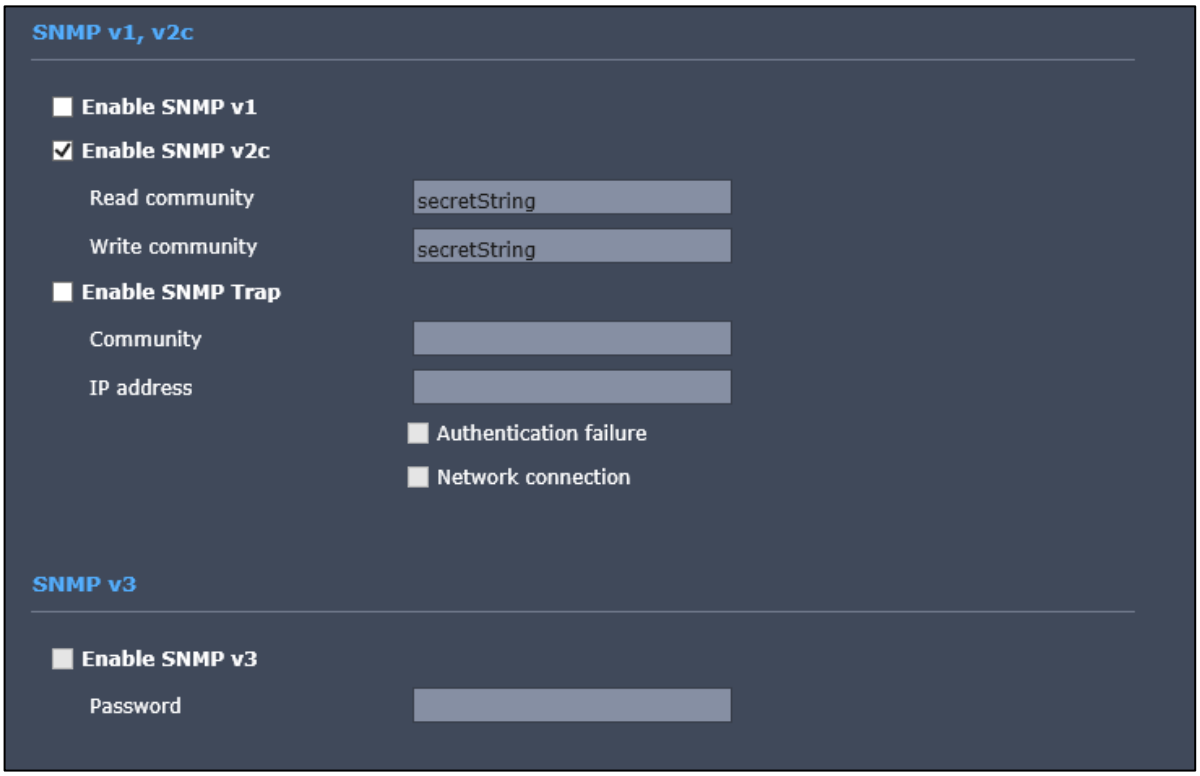
3) Write Community String을 추측하기 어려운 문자열로 변경

4) SNMP v1, SNMP v2c 적용

※ Community String은 영문자, 숫자를 포함한 8자리 이상의 구성을 권고



[Community String 변경]



[구버전 카메라의 Community String 변경]

WISENET

Hanwha Techwin Co.,Ltd.

13488 경기도 성남시 분당구 판교로 319번길 6 한화테크윈 R&D센터

TEL 070.7147.8771-8

FAX 031.8018.3715

http://hanwha-security.com

Hanwha Techwin