Hanwha Techwin

White paper

사이버보안

네트워크 장비 보안 강화

2020 년 11 월 17 일

Contents

Contents

1. 서론

네트워크를 통해 다른 시스템과 정보를 공유하는 장치와 시스템이 눈에 띄게 늘어나면서 세상은 점차 커넥티드 시대를 향해 나가고 있습니다. 이러한 트렌드 뒤에는 언제 어디에서나 네트워크에 연결하여 장치와 시스템을 간편하게 제어할 수 있기를 원하는 사람들의 바람이 자리잡고 있습니다.

하지만 네트워크 장치가 급증함에 따라 전례 없는 간편함을 누릴 수 있게 된 이면에는 보안 위험의 증가라는 부정적인 부분도 있다는 것을 간과할 수 없습니다. 각 장치가 네트워크 엔드 포인트의 역할을 하기 때문에 해커를 비롯한 악의적인 사용자가 이를 진입점으로 사용할 수 있는 가능성이 항상 존재합니다. 실제로 최근에 이목을 집중시켰던 데이터 유출 사례 중 대다수를 보면, 해커들은 데이터 유출을 방지할 수 있는 적절한 수준의 보안을 갖추지 못한 POS, *HVAC 또는 기타 네트워크 시스템을 통해 기업 네트워크에 침투할 수 있었습니다.

*HVAC : 공조기 (Heating, Ventilation and Air Conditioning)

IP 기반 영상감시 및 기타 솔루션이 인기를 모으면서 신규 구축 및 업그레이드를 위한 표준으로 인정 받고 있는 추세이지만 보안 시스템 역시 예외가 아닙니다. 해커는 해킹의 대상이 되는 네트워크 장치의 종류나 어떠한 기능을 하는지 구별하지 않습니다. 취약점으로 악용할 수 있는 잠재적 네트워크 진입점을 언급할 때 영상 감시 카메라와 기타 장치가 빠지지 않고 등장하는 것은 바로 이 때문입니다. 따라서 사용자는 네트워크, IP 카메라, 인코더, NVR 및 DVR의 보안 수준을 극대화할 수 있는 조치를 반드시 취해야 합니다. 장치 보안을 강화하여 무단 액세스를 차단하는 동시에 사용자의 영상 감시 시스템 및 전체 네트워크를 보호할 수 있는 모범 사례는 무수히 많습니다. 한화테크윈은 이러한 모범 사례를 잘 알고 있을 뿐만 아니라 사용자가 네트워크 보안 강화를 위해 중요한 조치를 보다 쉽게 취할 수 있도록 다양한 기술과 기능을 제품에 탑재하고 있습니다. 보안 시스템 운영자와 IT 담당자, 그리고 시스템 설치를 맡는 시스템 통합 업체는 이러한 기술과 기능을 검토하여 편의성과 허용 가능한 위험성 간의 균형을 유지해야 합니다.

1. 서론

본 백서에는 해당되는 경우 네트워크 카메라의 스크린 샷이 포함되어 있습니다. 대부분의 설정은 Wisenet Device Manager 소프트웨어를 사용하여 다수의 카메라에 일괄적으로 적용할 수 있습니다.

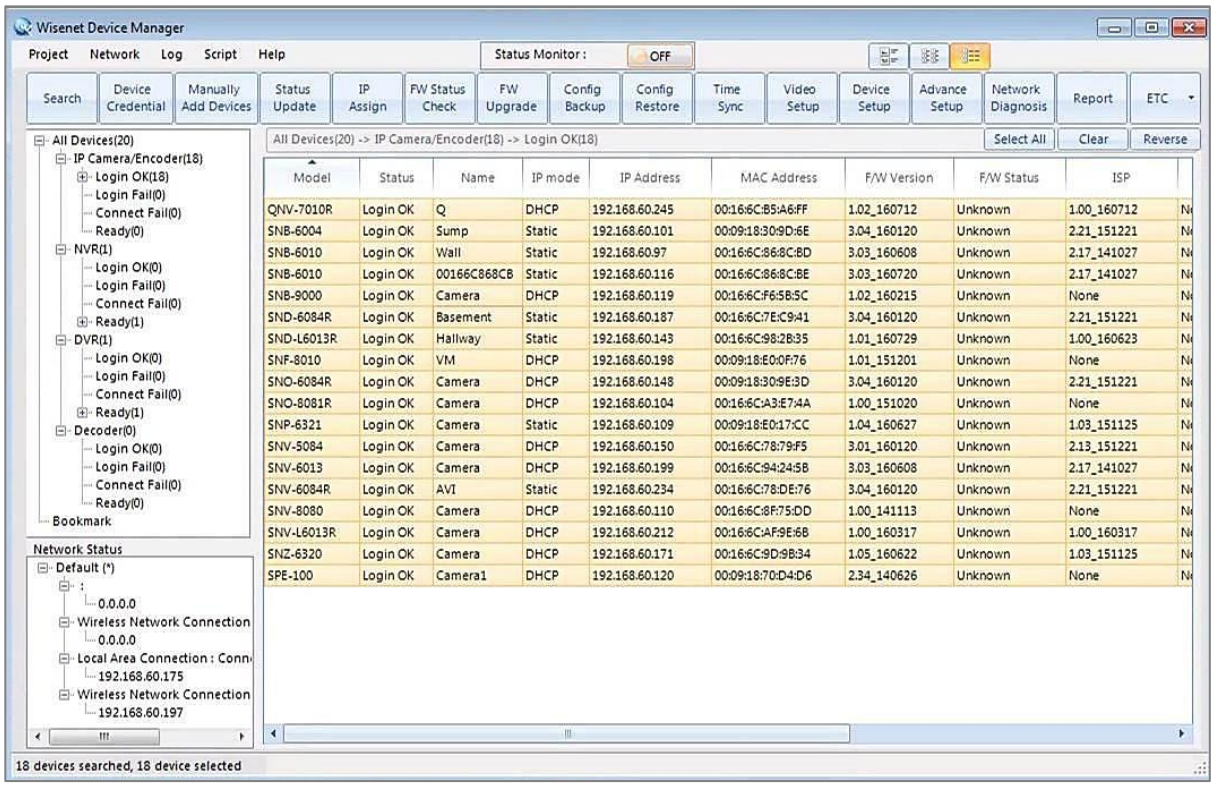


Figure 1. Wisenet Device Manager 사용 화면

2. 비밀번호 설정

스마트폰 잠금 해제, PC 로그인 및 이메일 확인에 이르기까지 비밀번호는 모든 일상에서 없어서는 안 될 부분입니다. 누구나 자신의 장치와 네트워크를 보호할 수 있는 강력한 비밀번호의 중요성에 대해 충분히 인식하고 있을 것 같지만 현실에서는 항상 그렇지만은 않습니다. 여기서 소개하는 모범 사례를 토대로 비밀번호 보안을 최고 수준으로 유지하는데 도움을 받을 수 있기를 바랍니다.

카메라, NVR, DVR 등의 장비에 초기 비밀번호가 있을 경우 보통 온라인이나 사용자 설명서에서 쉽게 찾아볼 수 있기 때문에 비밀번호 변경이 되어있지 않은 장비는 비인가자의 무단 접근을 허용하게 됩니다. 사용자는 반드시 초기 비밀번호를 그대로 사용하지 말고 고유의 비밀번호를 설정해야 합니다. 이러한 취약점을 사전에 차단하기 위해 한화테크윈의 모든 제품은 초기 비밀번호를 제공하지 않으며, 장비의 최초 사용 시 비밀번호를 반드시 설정한 후 사용할 수 있도록 되어 있습니다. 허나, 단순히 비밀번호를 변경하는 것만으로는 부족합니다. 사용자 인증을 요구하는 기능이나 애플리케이션들이 계속 늘어나면서 많은 사람들이 비밀번호 관련하여 간편함이라는 이유로 두 가지 실수를 하고 있으며, 특히 비밀번호를 만들 때 이 두 가지 실수에 모두 해당되는 경우가 빈번이 발생하고 있기 때문입니다.

첫 번째 실수는 모든 사용처에 동일한 비밀번호를 사용하는 것입니다. 예를 들어, 이메일 계정의 비밀번호를 누군가 해독하는데 성공하면 해당 비밀번호로 보호하고 있는 모든 정보에 접근할 수 있기 때문에 데이터 도난, 신원 도용 등이 발생할 가능성이 있습니다. 두 번째이자 가장 위험한 실수는 편의를 위해 이름이나 생년월일 등 타인이 유추하기 쉬운 단어나 숫자를 비밀번호로 사용하는 것입니다. 해커들은 비밀번호 해독을 위해 가능한 문자 조합을 자동으로 빠르게 대입하는 기술 등 강력한 도구를 사용하여 한층 조직화되고 지능화되었습니다. 이러한 도구들은 쉽고 간편하게 기억할 수 있는 비밀번호를 사용하는 사람들로 인해 지금까지 상당한 효과를 보였습니다.

2. 비밀번호 설정

또한, 방대한 양의 개인 정보가 온라인에 노출되면서 이름, 생일 또는 기타 유의미한 날짜를 사용한 비밀번호 역시 쉽게 무력화될 수 있습니다. 따라서 반드시 해독이 어려운 강력한 비밀번호를 사용해야 합니다. 이를 위해서는 문자, 숫자 및 특수 기호를 조합하여 사용하는 것이 바람직합니다.

필수 사항은 아니지만 각 장치마다 다른 비밀번호를 사용하거나 일부 네트워크 장비, 클라이언트 등 시스템 별로 다른 비밀번호를 사용하는 것이 바람직합니다. VMS나 기타 클라이언트 사용시 관리자 계정을 사용하지 않고 고유한 사용자 계정을 만드는 것도 권장됩니다. 이렇게 관리자 비밀번호가 네트워크를 통해 지속적으로 전송되는 것을 방지하면 중간에 유출될 가능성을 차단할 수 있습니다.

한화테크윈 제품은 8자의 문자로 구성된 비밀번호를 설정할 때는 대/소문자, 숫자 및 기호 등 적어도 3가지 이상의 문자가 조합되어야 하며, 10자 이상의 비밀번호 설정 경우에는 2가지 문자 조합이 필요합니다. 또한 4회 이상 반복되는 동일한 문자나 4회 이상 연속되는 문자는 암호로 사용할 수 없습니다. 비밀번호 설정 시, 특수 문자를 사용할 수 있으며, 비밀번호 최대 길이는 15자입니다.

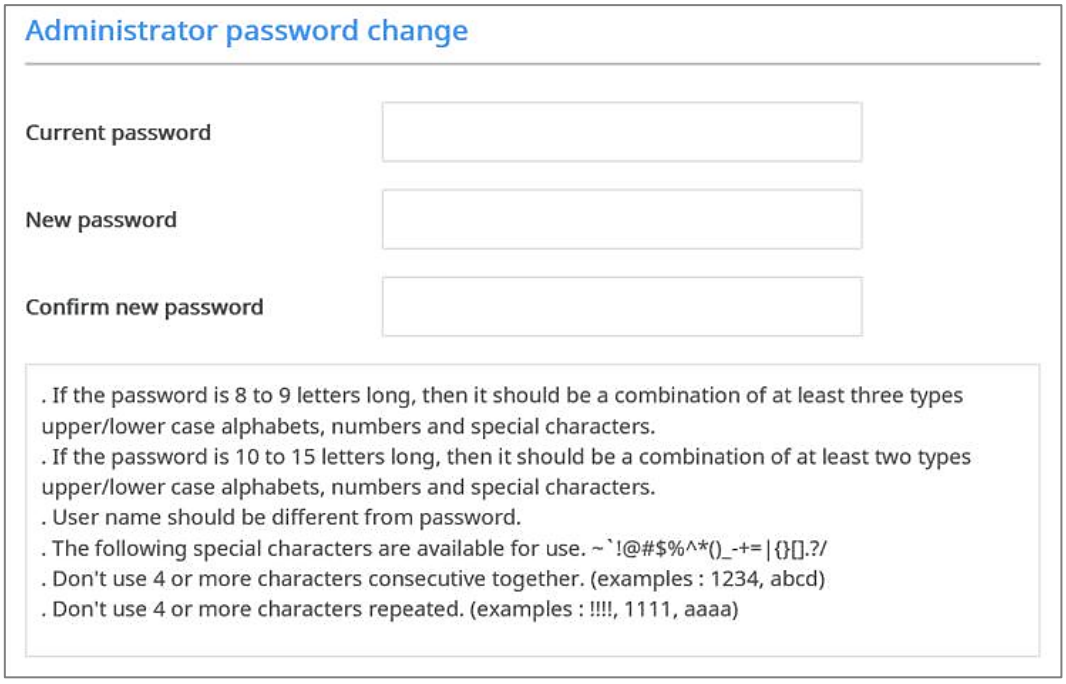


Figure 2. 카메라 비밀번호 설정 화면

3. 계정 권한 분리

사용자 계정 별로 권한을 제한하는 것은 해커의 접근을 차단하는데 매우 효과적입니다. 계정이 유출되더라도 설정 등을 비롯해 전체 시스템까지 영향을 미치는 것을 방지할 수 있고 사용자 별로 다른 계정을 사용하면 로그 분석이 보다 쉬워질 뿐 아니라 이를 통해 얻을 수 있는 정보도 더 유용해집니다. 한화테크윈의 카메라, 녹화 장치, VMS는 다양한 권한 및 수준별로 사용자 또는 사용자 그룹을 구분하여 생성할 수 있습니다.

3.1. 권한 최소화

권한 최소화는 필요한 최소한의 기능만 사용자에게 제공하는 것을 의미합니다. 예를 들어, 1년에 한번 설정 메뉴를 조작하는 사용자라면 계정에 대한 모든 접근을 허용하는 대신 웹 인터페이스를 통한 대체 사용자 로그인 기능을 제공하거나, 해당 작업을 더 높은 권한을 가진 사용자에게 맡기는 것이 좋습니다. 이렇게 하면 의도치 않은 구성 변경을 방지하는데 도움이 될 뿐만 아니라 높은 수준의 자격 증명을 네트워크에서 최대한 줄일 수 있습니다.

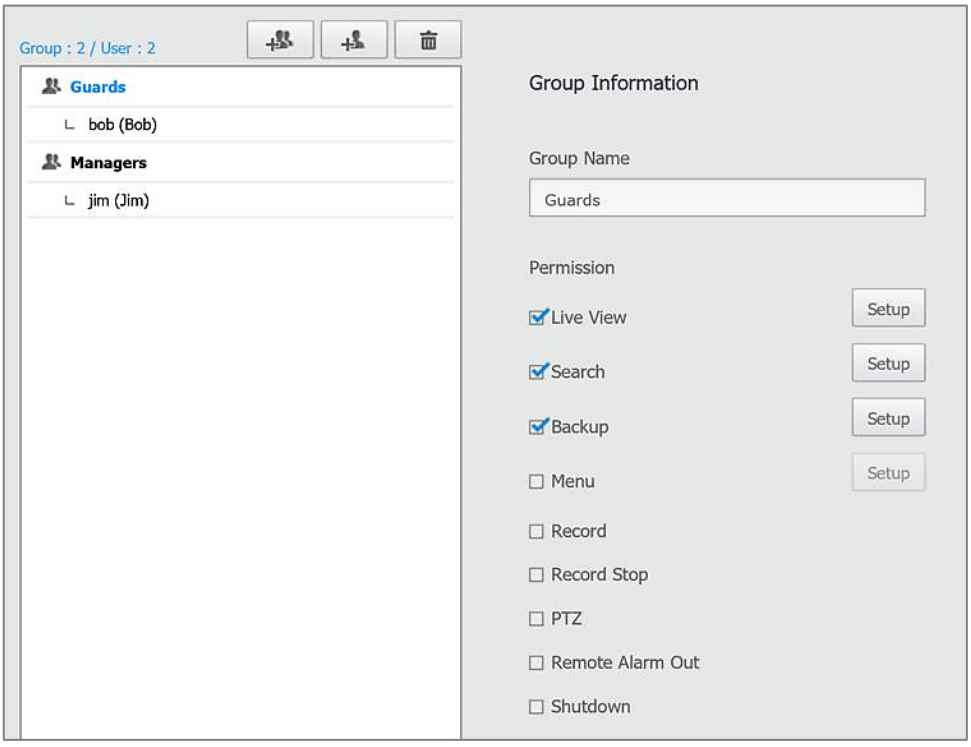


Figure 3. SSM 사용자 권한 설정 화면

3.2. 게스트 액세스

한화테크윈의 카메라는 사용자 이름과 비밀번호가 "guest"인 게스트 로그인 기능을 별도로 제공합니다. 이 게스트 계정은 권한이 제한적이며 기본적으로 비활성화되어 있으므로 설정 메뉴에서 따로 활성화해야 합니다. 이 계정은 액세스 사용을 제한하는데 이상적이지만 필요 없는 경우에는 비활성화 상태로 유지해야 합니다.

4. 인증 및 암호화

4.1. 다이제스트 인증과 일반 텍스트/베이직 인증 비교

사용자 인증 시 사용자 이름과 비밀번호를 네트워크를 통해 평문과 Base64 인코딩을 사용하여 전송하거나 HTTP 프로토콜에서 사용하는 베이직 인증을 사용하여 전송할 수 있습니다. 이러한 인증 방법은 자격 증명에 대한 개방형 액세스를 허용하기 때문에 임의의 누군가가 중간에 네트워크 트래픽 모니터링이 가능하며 장비에 접근할 수 있는 사용자 이름과 비밀번호가 고스란히 노출되게 됩니다.

이러한 취약한 인증 방법을 대신해서 해시 함수를 사용하여 데이터를 암호화하는 다이제스트 인증이 있습니다. 이렇게 암호화된 데이터는 장치에서 해시 처리된 자격 증명과 비교됩니다. 결과적으로 다이제스트 인증은 사용자 이름이 노출되는 작은 단점이 있지만 네트워크를 통해 실제 비밀번호를 전송하지 않기 때문에 안전한 사용자 인증 방식 중 하나입니다.

한화테크윈의 모든 제품은 다이제스트 비밀번호를 지원하며 안전하지 않은 베이직 인증은 제공하지 않습니다. 하지만 장치에 연결되는 모든 클라이언트에 동일하게 적용되는 것은 아닙니다. 따라서 모든 클라이언트가 동작하면서 일반 텍스트 또는 Base64 비밀번호로 전환되지 않도록 하는 것이 중요합니다.

4.2. SSL 암호화

보안을 효과적으로 유지할 수 있는 좋은 방법 중 하나는 SSL 암호화입니다. 이 방법을 사용하면 사용자 이름과 비밀번호는 물론 사용자 데이터를 전달하고자 하는 지점까지 안전하게 전송을 할 수 있으며 장치의 보안을 간편하고 경제적으로 강화할 수 있습니다.

SSL 암호화는 인증서를 설치하고 실행하는데 몇 초밖에 걸리지 않습니다. 이외에도 SSL 인증서는 상용 인증 기관에서 구매하거나 관련 법인을 통해 발급 받을 수 있으며 액세스할 때 인증서 보안 메시지가 표시되지 않도록 설정할 수도 있습니다. SSL 보안은 잠재적으로 안전하지 않은 네트워크 또는 클라우드에서 통신 채널을 강화하는데 효과적이긴 하지만 암호화가 필요하거나 지원되는 채널을 결정해야 합니다. 여기에는 카메라부터 NVR/VMS까지, 그리고 VMS부터 클라이언트까지 포함됩니다. 또한 자격 증명이 일반 텍스트로 전송되는 것을 방지하기 위해 SMTP 프로토콜을 사용하여 이메일을 전송할 때도 SSL 암호화를 사용해야 합니다. 이를 위해서는 SMTP 서버가 SSL/TLS를 지원해야 하며 사용되는 포트도 확인할 필요가 있습니다.

구성 옵션에서는 기본으로 제공되는 고유한 인증서 또는 공개 인증서를 선택하거나 인증서 및 키 파일을 설치하여 이름을 지정할 수 있습니다. HTTPS 옵션을 변경하면 카메라가 재부팅되며, 이후부터는 HTTPS 포트를 통해 암호화된 통신만 허용됩니다.

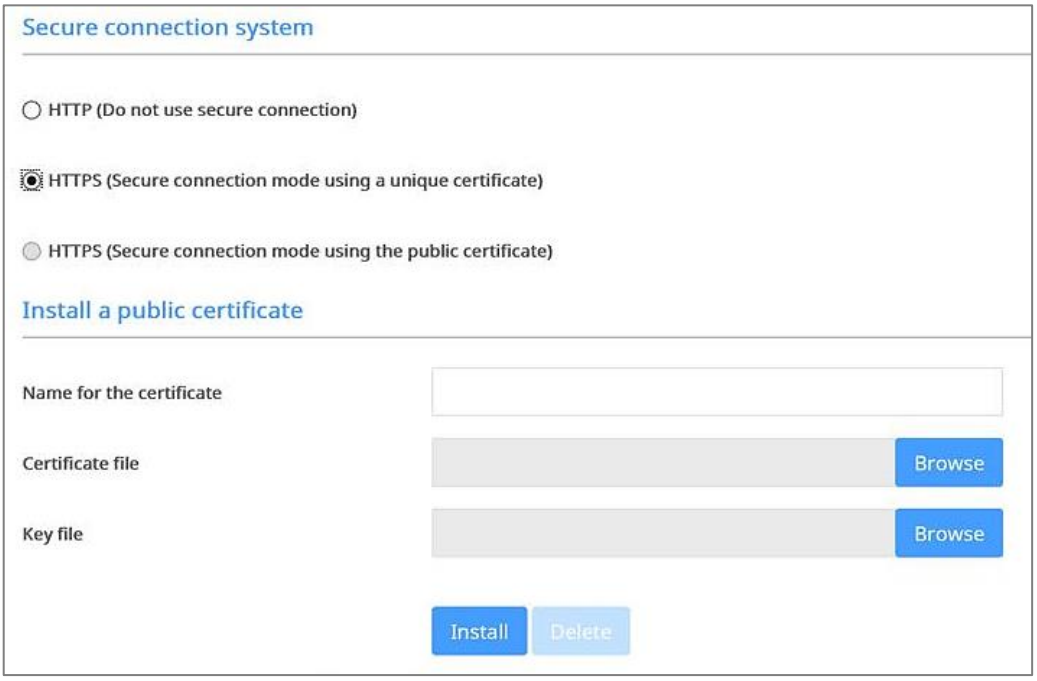


Figure 4. SSL 암호화 설정 화면

4.3. 클라우드 사용 최소화

클라우드 서비스를 사용하여 시스템을 녹화하거나 확인할 경우에는 엄청난 대역폭이 필요할 뿐만 아니라 보안 문제까지 발생할 수 있습니다. 클라우드에 장치를 연결하면 로그인 정보가 전송되기 때문입니다. 이 정보가 수집되거나 중간자 공격(MITM, Main in the middle)이 발생할 경우에는 자격 증명의 복호화 또는 재생으로 인해 무단 액세스가 가능해집니다. 또한 일부 클라우드 서비스는 SSL 암호화 또는 다이제스트 인증을 지원하지 않는 경우도 있습니다.

5.1. 물리적인 네트워크 분리

보안 네트워크의 안전성을 효과적으로 높이기 위해 흔히 사용되는 기술은 카메라와 녹화 장치를 기업 네트워크에서 물리적으로 격리하는 것입니다. 이렇게 하면 액세스가 어려워져 공격자가 액세스 권한을 얻지 못하게 됩니다. 또한 대부분의 NVR은 네트워크 인터페이스를 채택하고 있기 때문에 녹화 및 워크스테이션 액세스를 서로 다른 인터페이스에서 실행할 수 있습니다. 따라서 외부에 노출되어 보안 통제를 강화해야 하는 장치의 수가 줄어들게 됩니다.

5.2. VLAN

별도의 네트워크를 사용하지 않을 때는 가상랜(VLAN)을 사용하여 보안 네트워크를 기업 네트워크에서 격리하는 것이 바람직합니다. VLAN은 네트워크 스위치에서 운영되며 스위치 포트를 기준으로 트래픽을 격리합니다. 따라서 방화벽을 통해 시큐리티 장비를 네트워크상의 다른 장치에서 격리하여 보호할 수 있습니다. 특정 장치에 대한 액세스가 필요한 경우에는 방화벽 규칙을 생성하거나 장치를 VLAN에 추가하면 됩니다.

5.3. IP 필터링

IP 필터링은 네트워크 장치에 대한 액세스를 허용하거나 거부할 사용자를 명시적으로 지정하는 방법입니다. 여기에서는 IP 주소, 범위 또는 서브넷을 지정할 수 있습니다. 이렇게 하면 PC의 IP 주소에 따라 올바른 사용자에게만 장치 액세스를 허용하고 의도하지 않은 로컬 네트워크 또는 인터넷 액세스 시도는 거부할 수 있습니다. 한화테크윈의 장치에서는 IPv4 및 IPv6 IP 주소와 프리픽스(Prefix)를 입력하여 액세스를 거부하거나 허용할 수 있습니다.

IP와 프리픽스를 확인할 수 있도록 필터링 범위도 표시됩니다. 적용하기 전에 이 범위를 반드시 확인해야 접근이 거부되는 것을 방지할 수 있습니다. IPv4와 IPv6 항목은 각각 최대 10개까지 추가할 수 있습니다.

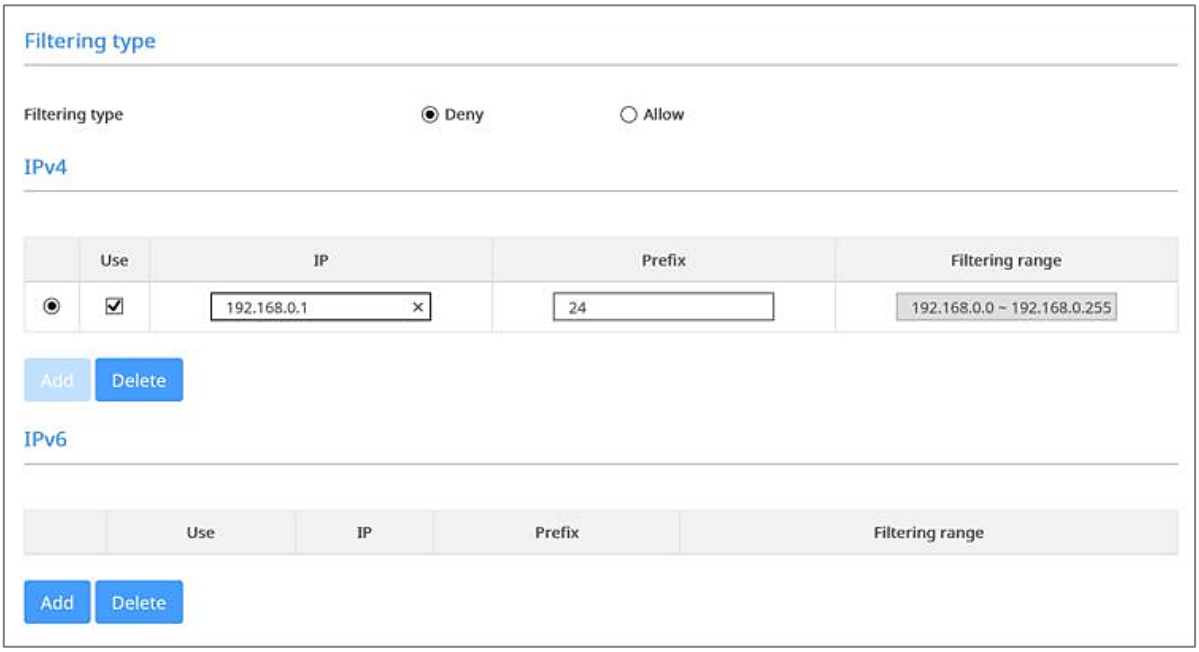


Figure 5. IP 필터링 설정 화면

5.4. VPN

원격지에서의 접근이 경우에는 VPN 솔루션을 사용하는 것이 가장 좋습니다. VPN을 사용하면 안전한 암호화 채널을 생성하여 사용자 이름이나 비밀번호 같은 정보가 유출될 수 있는 가능성을 미연에 방지할 수 있기 때문입니다. VPN 솔루션은 VPN 라우터 같은 전용 하드웨어를 비롯하여 클라이언트 PC에서 실행되는 소프트웨어 VPN이 필요할 수 있습니다.

5.5. 기본 포트 변경 및 미사용 포트/서비스/프로토콜 비활성화

오늘날과 같은 커넥티드 환경에서는 의도와 상관없이 많은 장치가 인터넷에 연결되기 때문에 해커 역시 스캔을 통해 이러한 장치를 검색할 수 있는 서비스가 많이 있습니다.

스크립트 키디즈(Script kiddies), 의도하지 않은 공격 및 부주의한 액세스를 포함하여 이러한 스캔 프로그램을 손쉽게 막으려면 인터넷 상에서 찾을 수 있는 정도의 잘 알려진 네트워크 장치의 기본 포트 번호를 다른 번호로 변경하는 것입니다. 특히, HTTP 웹 포트는 대부분의 장치에서 웹 브라우저를 통해 접근할

수 있도록 포트 80으로 기본 설정되어 있다는 점에서 더욱 중요합니다. 예를 들어, 이 포트를 8000으로 변경하면 웹 브라우저에 주소를 입력할 때 포트 번호의 추가 입력이 필요하기 때문에 단순한 스캔 프로그램이나 웹 브라우저에 주소를 직접 입력하는 공격자로부터 보호할 수 있습니다.

대부분의 시큐리티 장비는 일종의 컴퓨터처럼 운영 체제를 기반으로 동작하며, 한화테크윈은 미사용 서비스를 제거하거나 비활성화함으로써 불필요한 요소를 제거한 맞춤형 운영 체제를 제품에 적용해왔습니다. 하지만 몇몇 제조 업체들은 디버깅 등의 유지 및 관리 편의, 혹은 보안 인식 및 정책의 부재로 인해 미사용 서비스를 활성화 상태로 남겨두는 경우가 있습니다. 최근 타 제조사 장비의 해킹 사고들을 살펴보면 해커들이 전체 파일과 서비스에 대한 모든 명령 접근 권한을 부여하는 텔넷을 통해 장치에 접속하는 경우가 많았습니다. Windows 기반 녹화 플랫폼에는 지속적인 보안 업데이트와 패치 외에도 시간, 추적 및 인터넷 액세스 정보를 요구하는 서비스가 많습니다.

한화테크윈의 장치는 유용한 기능을 지원하는 프로토콜을 다양하게 이용합니다. 하지만 애플리케이션에 필요하지 않은 서비스는 모두 비활성화하는 것이 바람직합니다. 여기에는 멀티캐스트, DDNS(Dynamic DNS), QoS(Quality of Service), Bonjour, UPnP(Universal Plug and Play) 검색 및 포트 포워딩, 링크 로컬 주소, FTP(File Transfer Protocol), NAS(Network Attached Storage), 이메일 알림이 포함될 수 있습니다. 앞서 언급했듯이 사용자 별로 다른 계정을 이용하여 FTP, NAS 및 이메일 권한을 제한하는 것도 보안을 강화하는 좋은 방법입니다. 자동 IP 설정은 기본적으로 활성화되어 있지만, 다른 서비스는 모두 기본적으로 비활성화되어 있습니다.

5.6. RTSP

대부분의 VMS는 RTSP 프로토콜을 사용하여 비디오를 스트리밍합니다. 한화테크윈의 카메라는 인증 요청 없이 RTSP 비디오 연결이 가능한 옵션을 지원합니다. 이 옵션은 공개 시청 시 자격 증명이 노출되지 않도록 보장하고 인증이 지원되지 않는 제3자 서비스를 통합할 수 있다는 점에서 인터넷을 통한 스트리밍에 유용합니다. 한화테크윈의 카메라는 사용자 인터페이스에서 이 기능을 간편하게 활성화할 수 있습니다. 모든 비디오 스트림은 보안상 인증을 요구하도록 하는 것이 좋습니다. 공개 시청이 필요한 경우에는 서드파티 서비스 업체가 인증된 스트림을 수집한 후 카메라를 직접 공용 액세스로부터 격리한 다른 포털을 통해 공용 액세스 권한 제공이 가능합니다.

기본적으로 한화테크윈의 카메라는 사용자 인증 시 HTTP 프로토콜과 마찬가지로 RTSP 프로토콜에서도 다이제스트 인증 방법을 사용하기 때문에 비밀번호가 평문으로 노출되지 않습니다.

Figure 6. RTSP 인증 설정 화면

해커들이 가장 많이 사용하는 공격 방법은 무작위 입력 공격(Brute force attack), 서비스 거부(DoS, Denial of Service attack)와 버퍼 오버플로우입니다. 이 공격 방법들은 모두 유효성이 검증되었기 때문에 무단 액세스로부터 장치와 네트워크를 보호할 수 있는 적절한 해결 방안이 필요합니다. 한화테크윈의 카메라는 이 같은 공격을 효과적으로 차단할 수 있도록 다음과 같은 검증된 방법을 제공합니다.

6.1. 사용자 계정 잠금

해커들은 기기의 비밀번호를 찾기 위해 매우 빠른 속도로 무작위 값들을 기기에 입력합니다. 이러한 행위를 허용할 경우, 일정 시간이 지나면 기기의 비빌번호가 노출될 수 밖에 없는 위험이 있습니다. 보안을 향상시키기 위해 한화테크윈의 기기는 30초 이내에 5번 이상의 비밀번호 무작위 입력 공격(Brute force attack)을 차단하고 있으며, 단순히 모든 연결을 차단하는 방법이 아닌 기존의 인증된 연결은 유지하고 비인가된 연결 시도만 차단함으로써 무작위 입력 공격을 통해 유발될 수 있는 서비스 거부(DoS) 공격까지 예방하고 있습니다.

Figure 7. 비밀번호 입력 연속 5회 오류 시, 로그인 차단 화면

6.2. 버퍼 오버플로우 차단

해커들이 자주 사용하는 또 다른 공격 방법은 정보를 공개하거나 데이터베이스 또는 파일 시스템 같이 다른 기본 서비스로 전송하기 위한 명령을 장치에 전송하는 것입니다. 이러한 명령들은 파서(Parser) 또는 데이터베이스의 취약점을 악용하거나 인터페이스를 파괴하여 데이터베이스 서버, 운영체제 또는 파일 시스템으로 직접 전송됩니다. 한화테크윈의 장치는 웹 서버나 데이터베이스로 명령을 전송하기 전에 필터링하여 기본적인 주요 서비스에 해커가 접근하지 못하도록 차단함으로써 버퍼 오버플로우 및 직접 해킹에 따른 공격을 방지합니다.

6.3. 안전한 기기 배치

사용하는 기기가 비인가자에 의해 악의적으로 변경될 수 있는 상황이 발생할 수 있는데, 다음과 같은 방법으로 이러한 상황을 예방할 수 있습니다.

첫째, 네트워크 장비를 함체에 넣어 잠그거나 잠금 기능이 있는 네트워크 플러그 사용하는 방법이 있습니다. 이 방법으로 인가되지 않은 기기들이 스위치 등의 네트워크 장비에 접근하는 것을 물리적으로 막을 수 있습니다. 그러나, 침입자가 강제적으로 잠금 장치를 망가트릴 수 있기 때문에 완벽한 방어 기술이 아니므로 다른 종류의 네트워크 보안 기술과 병행으로 사용하여 시너지를 내는 것이 효과적입니다.

둘째, 스위치에 연결된 기기에 대하여 포트 보안(port security)을 하는 방법이 있습니다. 이 방법은 스위치의 특정 포트에 허가된 특정 기기만 접속할 수 있게 하는 것을 말합니다. MAC 필터링이나 802.1x 인증서 기반 접근 제어를 사용하는 방법이 있습니다.

셋째, 기기에 적절한 하우징 기법을 적용하여 사용자의 기기에 물리적으로 쉽게 접근하는 것을 방지하는 방법이 있습니다. 네트워크와 전원 케이블이 전선관을 통하거나 벽이나 천정을 통해서 기기로 바로 연결되면 케이블이 탈취되지 않고 안전하게 관리가 가능합니다. 한화테크윈의 반달돔(Vandal Dome) 카메라 역시 이러한 케이블에 대한 물리 보안의 해결 방안이 될 수 있습니다.

6.4. 녹화 연속성 보장

절도범들은 침입 시 영상 증거를 인멸할 목적으로 녹화 장치나 서버를 훔치거나 파손하는 경우가 종종 있습니다. 이를 막기 위한 한 가지 방법은 카메라마다 SD 카드를 사용하는 것입니다. 녹화 유지 기간이 비교적 짧기는 하지만 녹화 이중화 기능을 지원하기 때문입니다. 이외에도 NVR, VMS에 장애가 발생하거나 의도적이든 우발적이든 네트워크가 중단되는 경우에도 한화테크윈의 카메라는 물리적 네트워크 계층의 연결 해제를 자동적으로 감지하여 전원이 계속 공급되고 있는 한 SD 카드에 계속해서 녹화할 수 있습니다.

구성 옵션으로는 SD 카드 기능 활성화/비활성화, Full/I-Frame/None에 따른 연속/이벤트 녹화, 이벤트 전후 녹화 지속 시간, 녹화 파일 형식(AVI/STW), 덮어쓰기, 자동 삭제/지속 시간, 일반 녹화 예약 및 SD 카드 파일 시스템이 있습니다. 녹화할 때는 프로파일 또는 코덱을 제한 없이 선택할 수 있습니다.

또한, SD 카드 대신 NAS를 구성하거나 SD 카드는 장애 조치를 위한 선택적 백업 녹화 미디어로 사용하고 NAS를 기본 녹화 장치로 구성할 수도 있습니다. NAS 녹화는 IP 주소, 사용자 ID, 비밀번호 및 기본 폴더가 추가되는 것을 제외하고 구성 옵션이 동일합니다.

6.5. 기기에 대한 물리적 접근 차단

네트워크 시큐리티 장비에 대한 물리적인 접근은 무엇보다 중요합니다. 물리적 접근 시 대부분의 장치에서 초기화가 가능하기 때문에 권한이 없는 사용자가 새로운 설정을 구성할 수 있습니다. DID(Defense in Depth) 보안 모델에 따르면 네트워크 장치는 함부로 접근하지 못하도록 설치하는 것이 중요하기 때문에 접근 제어 및/또는 비디오 보안 모니터링 기능 등을 사용하는 것이 좋습니다. 이렇게 하면 보안 계층이 다중화되어 단일 메커니즘에 의존하지 않아도 됩니다.

예를 들면, 스위치의 비어있는 포트에 네트워크 케이블을 연결하여 내부 네트워크에 접근이 가능하므로 사용하지 않는 스위치 포트를 비활성화시킴으로써 인가되지 않은 기기의 접근을 예방할 수 있습니다. 스위치의 특정 포트를 비활성화시키는 기능은 스위치에서 기본으로 제공하는 옵션이므로 낮은 비용으로 어렵지 않게 구현이 가능합니다.

다만, 이 방법은 기존에 연결되어 있는 인가된 기기를 스위치에서 제거하고 새로운 비인가 기기를 연결하여 접근하는 방법의 경우에는 접근을 막을 수 없다는 것이 단점입니다. 이러한 단점을 보완할 수 있는 방법으로 802.1x 인증서 기반 접근 제어 방식을 사용하는 것을 추천합니다.

6.6. 802.1x 인증서 기반 액세스 제어

대부분의 건물에서는 네트워크 단자에 접근하거나 카메라의 전원 플러그를 뽑을 수 있으며 케이블을 조작하여 이더넷 네트워크 시설에 대한 액세스 권한을 얻을 수도 있습니다. 802.1x 표준은 이러한 방식의 접근을 방지할 수 있습니다.

802.1x 표준은 포트 기반 네트워크 액세스 제어를 지원해 보호 중인 네트워크에 액세스하려는 장치에 대한 인증 절차를 수행할 수 있습니다. 따라서 장치마다 식별 인증서를 설치해야 하며 유효하지 않은 장치를 통해 네트워크에 접근하려고 하면 액세스가 거부됩니다.

Wisenet Device Manager를 사용하면 카메라마다 일일이 설정할 필요 없이 네트워크 내 카메라들의 802.1x 인증을 간편하게 활성화하고 인증서를 배포할 수 있습니다. 구성 옵션으로는 EAP 유형 및 EAPOL 버전 선택, 사용자 ID 및 비밀번호 설정, 인증서/키 설치 등이 있습니다.

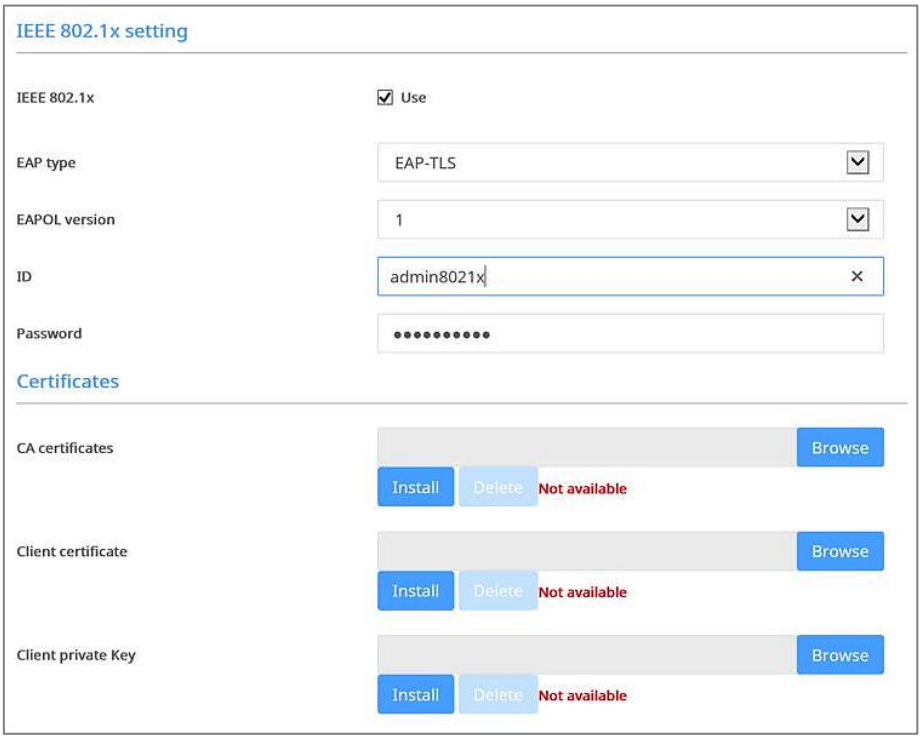


Figure 8. 인증서 설치 메뉴 화면

6.7. 전원

UPS는 정전, 절전 및 계획된 차단을 비롯하여 우발적이거나 악의적인 전원 차단 시 네트워크 장치의 전원 공급을 유지하는 동시에 순간 전력 급증으로 인한 손상을 방지할 수 있습니다. 대부분의 IP 카메라는 PoE 전력 예산이 초과할 경우를 대비하여 전력원 이중화 기능을 제공하며, 모델에 따라 PoE 및 저전압 12v DC/24v AC를 전력원으로 사용할 수 있습니다. 대부분의 네트워크 스위치도 장치 유형(전화기, 카메라, WAP 등)이나 전력 부족 시 포트 중요도를 나타내는 우선 순위를 지정할 수 있습니다. 또한, 관리 목적으로 UPS가 네트워크에 연결된 경우에는 안전성을 확인하고 보안 업데이트를 설치해야 합니다. UPS 같이 모니터링을 목적으로 LAN이나 인터넷에 연결된 보조 장치를 통해 네트워크에 접근하려는 공격 사례도 있었기 때문입니다.

6.8. 네트워크 관리

보안을 유지하기 위해 네트워크 관리자는 카메라와 기타 장치를 설치한 후에도 여러 작업을 지속적으로 실시해야 합니다. 시스템 개선 및 일관된 설정 관리, 소프트웨어 업데이트, 소프트웨어의 기업 보안 표준 준수 등이 있으며 그 중에서도 특히 모든 변경 사항에 대한 검토가 매우 중요합니다.

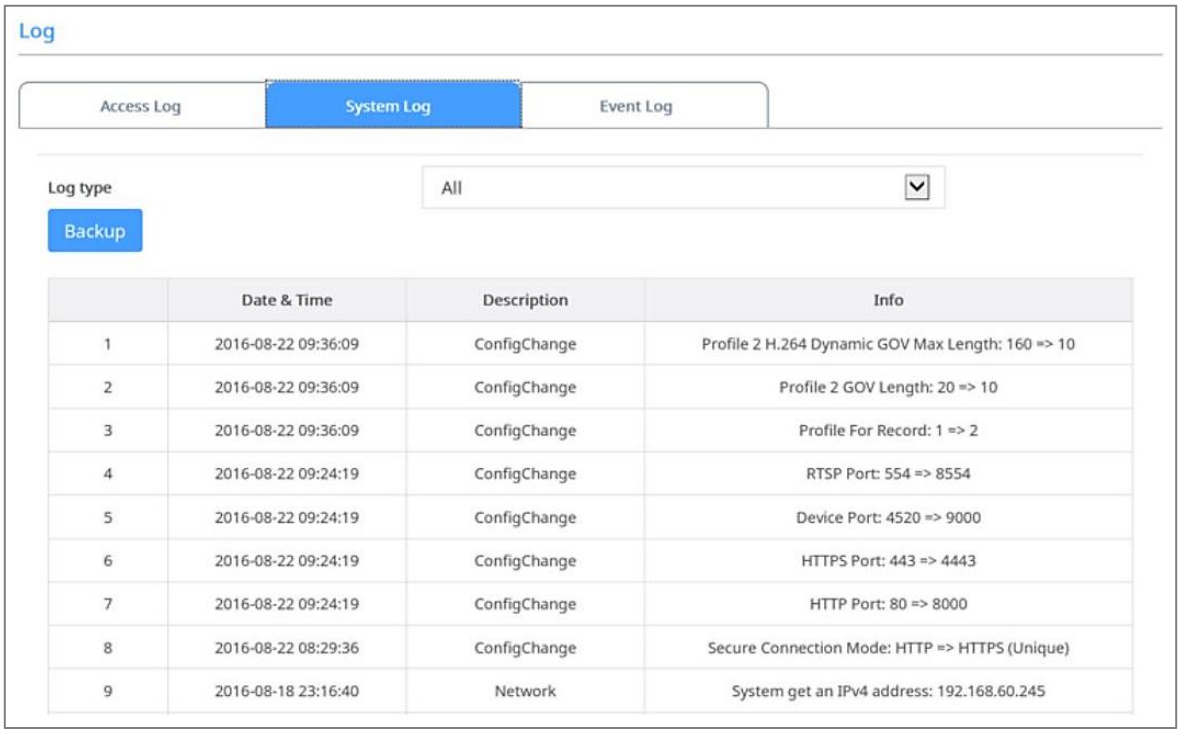
한화테크윈은 앞서 설명된 바와 같이, 장치를 엄격히 관리하고 해커로부터 네트워크를 보호하는 것이 매우 중요한 역할이라는 것을 정확하게 인식하여 강력하고 포괄적인 전략을 수행하고 있습니다.

6.9. 장치 로그 확인

한화테크윈의 카메라는 모든 장치 설정 변경 사항을 기록하기 때문에 로그를 확인하여 어떤 내용이 변경되었으며 누가 변경했는지를 파악하는 것이 가능합니다. 대부분의 로그 항목에는 롤백이 용이하도록 이전 설정과 새로운 설정이 모두 포함되어 있을 뿐만 아니라 공장 초기화할 경우에도 이러한 로그가 그대로 유지되도록 되어 있습니다.

로그를 초기화하지 못하도록 하는 기능은 해커가 자신의 침입을 감추기 위해 고의로 기기를 초기화할 경우를 예방해주어 비인가자의 침입 경로 분석 및 추적에 매우 유용하게 사용될 수 있습니다. Wisenet Device Manager를 사용하면 여러 장치에서 로그를 한 번에 간편하게 다운로드 할 수 있습니다.

설정이 유효한지 검증할 수 없는 경우에는 공장 초기화를 진행하여 올바른 기본 설정으로 되돌릴 수 있습니다. 한화테크윈의 카메라에서는 전원이 켜진 상태에서 공장 초기화 버튼을 5초 동안 누르고 있으면 기본 설정으로 바뀝니다. 카메라를 초기화한 후에는 반드시 IP 주소를 재구성하고 기본 관리자 비밀번호를 설정해야 합니다. 공장 초기화를 진행하더라도 필요에 따라 모든 'IP & 포트' 및 '네트워크' 설정을 유지할 수 있습니다.



	Date & Time	Description	Info
1	2016-08-22 09:36:09	ConfigChange	Profile 2 H.264 Dynamic GOV Max Length: 160 => 10
2	2016-08-22 09:36:09	ConfigChange	Profile 2 GOV Length: 20 => 10
3	2016-08-22 09:36:09	ConfigChange	Profile For Record: 1 => 2
4	2016-08-22 09:24:19	ConfigChange	RTSP Port: 554 => 8554
5	2016-08-22 09:24:19	ConfigChange	Device Port: 4520 => 9000
6	2016-08-22 09:24:19	ConfigChange	HTTPS Port: 443 => 4443
7	2016-08-22 09:24:19	ConfigChange	HTTP Port: 80 => 8000
8	2016-08-22 08:29:36	ConfigChange	Secure Connection Mode: HTTP => HTTPS (Unique)
9	2016-08-18 23:16:40	Network	System get an IPv4 address: 192.168.60.245

Figure 9. 시스템 로그 중 설정 변경 항목 확인

6.10. 정기적인 펌웨어 업데이트

해커들은 오랫동안 보안 업데이트를 설치하지 않은 이전 버전 소프트웨어의 취약점을 악용하기 위해 호시탐탐 기회를 노립니다. 일단 취약점이 발견되면 온라인으로 급속히 전파되기 때문에 불특정 개인이 이전 펌웨어 버전의 장치는 물론이고 더 나아가 네트워크까지 쉽게 침투할 수 있는 경로가 열리는 셈입니다. 소프트웨어 공급 업체들은 이러한 사실을 인식하고 문제를 개선한 업데이트를 비롯하여 무단 액세스를 방지할 수 있는 패치를 지속적으로 배포하고 있습니다.

한화테크윈의 모든 장치에 사용되는 펌웨어에는 관리자가 최신 버전을 운용하기 위해 참조할 수 있는 업데이트 목록이 포함되어 있습니다. 펌웨어는 최신 상태 여부를 확인한 후 정기적으로 업데이트를 계속하는 것이 좋습니다. 대부분의 인스톨러도 시스템 설치에 앞서 펌웨어 최신 상태 확인 및 업데이트를 진행하는 추세입니다.

Wisenet Device Manager를 사용하면 모든 장치의 펌웨어 버전 및 최신 버전 여부를 한 번에 확인할 수 있으며, 클릭 몇 번만으로 편리하게 펌웨어를 다운로드하여 설치할 수 있습니다.

6.11. 펌웨어 암호화

대부분의 보안 장비 제조사들은 사용자로 하여금 기능 추가, 버그 개선 및 보안 업그레이드를 할 수 있도록 자사의 사이트를 통하여 펌웨어를 제공하고 있습니다. 이렇게 개선을 위해 제공되는 펌웨어 또한 해커들의 타겟이 될 수 있습니다.

펌웨어 안에는 우리가 생각하는 것 이상으로 매우 중요한 정보들이 포함되어 있습니다. 예를 들어, 사용자 계정을 확인하는 알고리즘, 중요 정보를 암호화 하기 위해 사용하는 암호화 알고리즘과 키 정보, 운영 시스템 파일이나 중요 웹서비스 URL 등이 노출될 수 있고, 백도어(Back Door)를 침투시킬 수 있는 약점이 노출될 가능성도 있습니다. 이런 약점을 이용해 백도어를 포함시켜 변조된 펌웨어의 유포와 업데이트가 가능하게 되며, 이를 통해 해커에게 기기의 제어권이 넘어가게 되면 다른 주변 시스템 공격의 전초 기지로 사용될 수 있습니다.

네트워크 시큐리티 장비를 포함한 대부분의 임베디드 기기들은 현재까지 펌웨어 보안을 위해 특별한 안전장치를 마련하지 않고 있습니다. 한화테크윈은 이러한 펌웨어 보안과 안전한 업그레이드를 위해 암호화된 펌웨어를 배포하고 있으며, 업계에서 권고하는 안전한 암호화 알고리즘을 사용하고 있으므로, 새로운 펌웨어가 배포되면 최신의 펌웨어로 안심하고 업데이트 해주시면 됩니다.

6.12. 비디오 포맷

대부분의 보안 장비는 산업 표준, 개방형 비디오 포맷 및 고유 비디오 포맷을 지원합니다. 사용자 입장에서는 자신이 즐겨 사용하는 미디어 플레이어로 비디오 파일을 열 수 있다는 점에서 개방형 비디오 포맷이 이상적으로 보일 수도 있습니다. 하지만 보안 애플리케이션은 편집, 수정 또는 조작이 불가능한 포맷을 필요로 합니다. 이는 비디오 파일을 다운로드 할 때 비디오 인증을 비롯해 조작되지 않았음을 보장할 수 있는 메커니즘이 반드시 필요하다는 의미에서 필수적입니다. 하지만 개방형 포맷으로는 이를 구현할 수 없습니다.

한화테크윈의 비디오 포맷은 이처럼 중요한 보호 기능을 지원할 뿐만 아니라 복잡한 비밀번호를 선택적으로 적용하여 비디오를 증거로 사용할 수 있도록 지원합니다. 한화테크윈 NVR/VMS에서 SEC 파일 포맷으로 추출한 비디오 파일은 재생에 필요한 플레이어가 자동으로 포함되어 있어 별도로 플레이어를 설치할 필요가 없으며 사용자가 SEC 파일을 더블 클릭함으로써 간단하게 비디오 파일을 재생시킬 수 있습니다. SEC 파일로 저장 시 비디오의 해쉬 정보를 프레임마다 같이 저장하여 해당 비디오의 변조 여부를 확인할 수 있는 워터마킹 기능을 제공하며 비밀번호를 설정하여 저장하면 암호화된 SEC 포맷으로 저장되기 때문에 해당 비디오 파일이 유출되더라도 개인 정보를 보호할 수가 있습니다.

한화테크윈의 VMS인 SSM에서는 워터마킹 기능뿐 아니라 디지털 서명을 추가 지원하며 전체 비디오 영상에 대한 해쉬 정보를 사용하여 서명 및 검증함으로써 해당 비디오의 변조 여부 및 출처를 확인할 수 있습니다. 해당 워터마킹과 디지털 서명에 대한 검증은 백업 뷰어 도구를 사용하여 확인이 가능합니다.

녹화 장치의 웹 브라우져에서는 AVI 파일 포맷으로도 추출이 가능한데 해당 비디오 파일은 개방형 비디오 포맷이므로 범용 미디어 플레이어로 재생이 가능합니다. 한화의 IP 카메라는 한화의 고유한 파일 포맷(STW)으로 비디오를 저장할 수 있으며, 웹 브라우져를 통해 내보내기가 가능합니다. 또한 별도의 SD 카드 플레이어를 사용하여 재생할 수도 있으며, AVI 파일 형식으로 변환이 가능합니다.

6.13. 오픈플랫폼 애플리케이션

대부분의 한화테크윈 카메라는 타사 애플리케이션을 설치하여 번호판 식별, 리테일 비즈니스 인텔리전스, 피플 카운팅 등의 기능을 추가할 수 있습니다. 카메라에서 애플리케이션을 실행할 때는 설치된 애플리케이션과 소프트웨어 패키지 소스를 알아두는 것이 중요합니다. 한화테크윈 카메라는 애플리케이션 설치 시 해당 애플리케이션에서 요구하는 권한을 표시합니다. 이 정보를 주의해서 검토하고 설치와 사용 여부를 판단해야 합니다.

애플리케이션의 유효성을 검증할 수 없거나 그 목적을 알 수 없는 경우에는, 즉시 설치를 중단, 제거한 후 신뢰할 수 있는 파트너의 애플리케이션을 이용하시길 바랍니다. 구성 옵션으로는 자동 시작 설정, 우선 순위 수준, 애플리케이션 시작/정지, 애플리케이션 설치/제거, 애플리케이션 웹 페이지 실행 등이 있습니다.

7. 결론

오늘날과 같은 커넥티드 환경에서 특정 개인이나 그룹이 네트워크의 취약점을 악용하여 보안을 무력화하려는 시도는 끊이지 않을 것입니다. 네트워크를 통해 다수의 장치에 접속해서 얻을 수 있는 편리함은 커다란 이점이지만 이러한 장치들을 통해 비인가자가 네트워크에 무단으로 접근할 수 있는 가능성이 증가한다는 것 또한 현실입니다. 따라서 해커들이 이러한 장치들을 진입점으로 악용하지 못하도록 방지하려면 보안 강화가 필수적입니다. 앞서 살펴본 모범 사례들을 활용하면 네트워크 영상감시장치와 시스템을 진입점으로 악용하지 못하도록 보호할 수 있을 뿐만 아니라 주요 기능의 무결성과 연속성을 유지함으로써 사람과 자산을 안전하게 지켜낼 수 있는 밑바탕이 될 것입니다.

최종 사용자, IT 담당자, 설치 업체 및 시스템 통합 업체 간의 구체적인 정보에 기반한 대화는 각 기업 또는 기관에 적합한 최적 보안 솔루션을 찾기 위한 열쇠가 될 것이며, 여러 모범 사례들은 네트워크 보안을 중요하고 신중하게 여기는 기업과 논의를 시작하는 출발점으로서도 훌륭한 역할을 할 것입니다.

한화테크윈은 보안 전담팀을 운영하여 제품 개발 단계에서부터 보안성을 사전 점검하고, 전문 기관 의뢰를 통해 위험 진단을 실시하고 있습니다. 빈틈 없는 보안을 위해 사용자 인증, 데이터 베이스, 펌웨어의 암호화 및 백도어 제거 정책을 전 제품에 적용하고 있으며, ID/패스워드 정책 또한 업계에서 가장 강력한 수준으로 적용하고 있습니다.

WISENET

13488 경기도 성남시 분당구 판교로 319 번길 6
한화테크윈 R&D 센터
TEL 070.7147.8771-8
FAX 031.8018.3715
http://hanwha-security.com

Hanwha Techwin