사이버 보안을 위한 펌웨어 장기 지원 정책

2024.09

V3.1

목차

개정이력

버전	개정일자	개정내용	비고
v1.0	2018. 6. 5	사이버 보안 장기 펌웨어 지원 정책 제정	
v1.1	2018. 7. 11	업데이트 단계 수정	
v2.0	2019. 10. 23	카메라/저장장치 적용대상 수정, 카메라 버전관리 추가	
v2.2	2023. 4.12	사명 변경으로 템플릿 수정	
v3.0	2024. 7. 12	펌웨어 개선 및 수정사항 추가, 용어 수정	
v3.1	2024. 9. 10	버전규칙 수정, 용어 수정(카메라 → 장비)	

1. 소개

최근 사이버 보안에 대한 인식이 높아짐에 따라, 한화비전은 사이버 보안 이슈에 빠르게 대응하고 고객이 안심하고 제품을 이용할 수 있도록 사이버 보안 펌웨어 장기 지원 정책을 수립하였습니다.

당사의 네트워크 장비 사이버 보안 펌웨어 장기 지원 정책은 펌웨어 개선 활동 뿐만 아니라, 보안 취약점들에 대한 대응 활동과 보안 사고 예방을 위한 제품 보안 품질 개선 활동을 포함하고 있습니다. 또한 사이버 보안을 강화하고 경쟁력 확보를 위하여 차별화 보안 솔루션 개발 활동과 각종 보안 인증 획득 활동을 포함하여 운영하고 있습니다.

펌웨어 장기 지원 정책은 아래 기준부터 적용됩니다.

■ 네트워크 카메라

☞ 펌웨어 버전 1.30 이상

[네트워크 카메라 버전 체계]

MODEL NAME_##.##.##_YYMMDD

예) XND-8080R_1.31.00_20190905

- 네트워크 카메라 버전이 1.30 이전이거나,
  버전 체계가 '0.00.YYMMDD'이라면 해당 정책 제외

■ 저장장치

☞ 펌웨어 버전 3.00 이상

[저장장치 버전 체계]

MODEL NAME_##.##.##_YYMMDD

예) HRX-1621_3.01.00_20190905171108

- 저장장치 버전이 3.00 이전이거나,
  버전 체계가 '0.00.YYMMDD'이라면 해당 정책 제외

※ 자세한 내용은 '5.부록' 참고

2. 사이버 보안 펌웨어 업데이트

한화비전은 다음과 같이 4 단계를 통해 사이버 보안이 강화된 펌웨어 업데이트를 제공합니다.

2.1. 제품 출시 전 단계

한화비전은 제품에 사용되는 오픈소스 소프트웨어의 안정성 확보를 위해 최신 버전의 상태를 유지합니다. 또한, 주기적으로 공인된 외부 전문업체의 침투테스트와 펌웨어에 대한 종합적인 점검 및 개선활동을 통해 출시 시점에 완벽한 보안성 확보에 최선을 다하고 있습니다.

2.2. 적극적 펌웨어 개선 단계(제품 출시 ~ 2 년)

제품 출시 후 2 년 동안 접근통제 및 영상정보 보호(기밀성, 무결성, 가용성)관련 사이버 보안 취약점 개선을 위한 적극적인 펌웨어 업데이트 활동을 지속합니다.

보고되거나 알려진 취약점 뿐만 아니라 정기적인 자체 침투 테스트 및 보안점검 활동을 통하여, 알려지지 않은 보안 위협이나 잠재되어 있는 위험이 악용되지 않도록 사전 예방 활동도 함께 수행합니다. 다음은 적극적 펌웨어 개선 활동의 구체적인 사례입니다.

1) 보안 취약점 대응 활동

외부에서 접수된 보안침해사고(보안취약점)는 당사의 보안침해사고 사후대응규칙에 따라 신속히 대응 및 사후 관리되고 있습니다. 당사의 보안 취약점 공지 정책에 따라 개선된 펌웨어가 빠르게 고객에게 제공됩니다.

[참고] 보안취약점 공지 정책

2) 제품 보안 품질 개선 활동

당사는 잠재되었을 지 모를 보안 취약점 개선을 위하여 개발자 주도 보안 점검 활동을 상시 실시하고 있으며, 역공학 도구를 이용한 취약점 확인 및 정기적인 외부 전문가(화이트 해커)를 통해 침투테스트를 수행하고 있습니다. 그리고 그 결과는 구체적인 보안 테스트 기준 개발로 이어지며, 모든 제품은 반드시 보안 테스트를 통과해야 출시가 가능합니다.

[참고] 사이버 보안 기술 백서, 네트워크 장비 보안 강화 가이드

2. 사이버 보안 펌웨어 업데이트

3) 차별화 보안 솔루션 개발활동

당사는 OpenSSL 과 같은 오픈 소스 S/W 를 통해 발생될지 모를 보안 취약점을 예방하기 위해, 네트워크 장비마다 고유한 기기 인증서와 개인키를 적용하여 통신 보안취약점의 근본적인 대응을 도모하고 있습니다.

또한 장기적으로 사용자 인증, 비디오 인증, 펌웨어 전자서명 등과 같이 네트워크 감시 장비의 차별화를 꾀할 수 있는 보안 솔루션을 확대 적용할 예정입니다.

4) 보안 인증 획득 활동

세계적으로 사이버 보안의 중요성이 커지면서, 보안 인증에 대한 관심이 높아지고 있습니다. 한화비전은 이러한 변화에 맞춰, 각종 사이버 보안 인증 획득을 통해 제품의 기밀성, 무결성 및 가용성을 검증 받아, 보안 위협에 대한 우려를 해소하고 제품 경쟁력을 확보하기 위해 노력하고 있습니다.

또한, 미국을 비롯한 전 세계에서 인정받는 보안 인증인 UL-CAP 과 FIPS 표준보안인증을 보유하고 있으며 FIPS 표준인증을 받은 TPM 과 보안 요소를 활용해 사이버 보안 위험으로부터 제품을 보호하고 있습니다. 진화하는 사이버 위협의 특성을 감안하여 세계적으로 신뢰성 있고 안정적인 사이버 보안 인증을 지속적으로 획득하는 활동을 통해 최고 수준의 제품보안을 확보하는 노력을 지속적으로 하고 있습니다.

2.3. 능동적 펌웨어 개선 단계(2 년 ~ 단종 전)

제품 출시 후 2 년에서 제품이 단종되기 전까지 접근통제 및 영상정보 보호 관련 사이버 보안 취약점 개선을 위한 능동적인 펌웨어 업데이트 활동을 수행합니다. 이 기간 동안, 외부 기관으로부터 보고된 보안 취약점 또는 잠재적인 공격 가능성이 있는 것으로 알려진 문제점들에 대한 개선을 반영하여 펌웨어 업데이트를 제공합니다.

당사는 외부 기관으로부터 보안취약점이 접수되면 보안침해사고 사후대응규칙에 따라 즉시 보안침해사고 대책 협의회를 소집하며, 취약점 내용 및 영향도 분석을 통해 최선의 방안을 마련하고 있습니다. 또한, 보안 취약점 공지 정책에 따라 개선된 펌웨어는 최대한 신속하게 배포하고 있습니다.

2. 사이버 보안 펌웨어 업데이트

2.4. 지속적 펌웨어 관리 단계(단종 후 ~5 년)

제품 단종 후 5 년까지 제품에 심각한 보안 문제를 발생시키는 취약점이 발생 시, 제품의 보안 안정성 유지를 지속하기 위해 보안이 강화된 펌웨어를 제공합니다.

확인된 문제는 이전 단계와 마찬가지로 보안침해사고 사후대응규칙에 따라, 신속하고 철저한 보안 취약점 분석을 통해 최선의 방안을 도출하여 개선된 펌웨어를 제공하게 됩니다.

3. 펌웨어 개선 및 수정 활동

한화비전은 제품 수명주기 동안 정기적으로 최소 1 년에 한 번 이상 업데이트를 지속적으로 지원합니다. 이러한 업데이트에는 사이버 보안 업데이트, 성능 향상, 버그 수정 및 새로운 기능이 포함됩니다.

제품 단종 후에도 아래 맺음말의 테이블처럼 주기적인 업데이트를 지원하여 당사 제품을 사용하는 고객에게 최고의 제품을 사용할 수 있도록 노력합니다.

4. 맺음말

한화비전은 제품 단종 후 최대 5 년까지 사이버 보안이 향상된 펌웨어를 업데이트하여 제공함으로써, 더욱 안전하고 신뢰할 수 있는 제품으로 고객에게 다가갈 것입니다.

아울러, 네트워크 카메라 및 저장장치 이외의 제품들에 대해서도 보안 취약점으로 인한 보안 위협에 노출될 가능성이 있다면, 공식적인 처리 절차를 거쳐 해당 제품들에 대해 보안 업데이트를 제공하여 우리 제품을 사용하는 고객들의 보안 피해를 줄이기 위해 노력할 것입니다.

유형	설명	EOL 후 지원
사이버 보안	심각한 취약성	5 년
중대한 버그	펌웨어 업데이트 외에는 개선 불가	3 년
경미한 버그	다른 개선 방안 존재	1 년
OS 업데이트	운영 체제 업데이트	1 년 * SoC 공급업체에서 제공하는 경우에만 해당
기능 요청	고객 기능 요청	1 년

5. 부록

■ 네트워크 장비 버전 규칙

한화 비전 네트워크 장비 버전은 신규 기능을 추가하거나 버그 수정을 위해 업데이트가 진행되며, 크게 플랫폼 버전과 제품 버전으로 나누어집니다.

✓ Platform: 한화 비전 장비의 플랫폼 릴리스 버전을 명시합니다.

Platform의 Major 버전은 한 자리 또는 두 자리 숫자로 표기하며, 한 자리 숫자 표기 시 앞자리는 생략됩니다.

- Major: 플랫폼의 구조 변경 및 주요 기능 변경사항 반영–
- Minor: 전 모델에 적용되는 신규 기능과 통합된 변경사항 반영

✓ Product: 한화 비전 장비의 모델별 릴리스 버전을 명시합니다.

- Major: 모델별 주요 기능 추가 및 변경 사항 반영
- Minor: 모델별 보고된 버그 및 잠재적인 문제 수정

<버전 표기 예>

23.01.00 버전의 의미는 플랫폼 버전 23.0 과 제품 버전 1.00 으로 구분되며, 플랫폼의 23.0 버전을 제품에 처음 반영한 것을 나타냅니다.

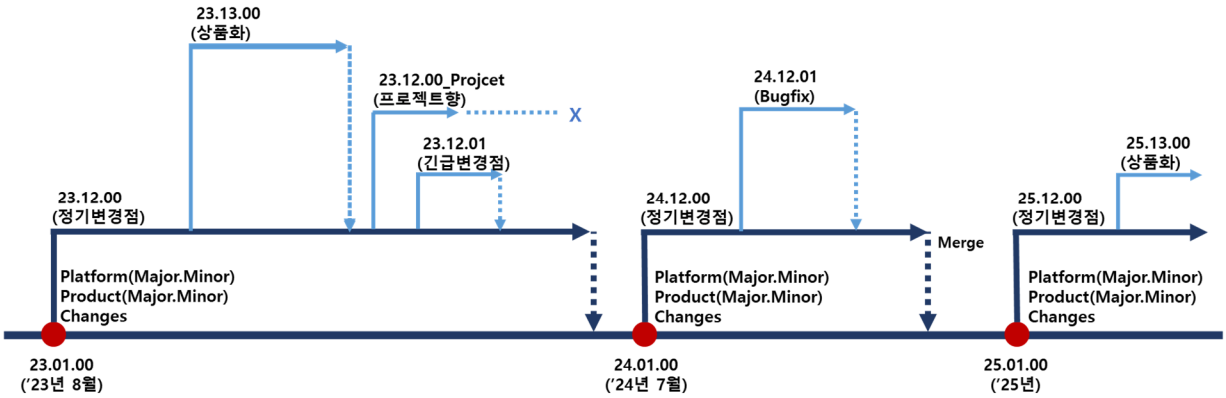
23.02.01 버전의 의미는 플랫폼의 23.0 버전을 기반으로 2 번의 기능 추가와 1 번의 문제점이 수정되었음을 나타냅니다.

5. 부록

아래와 같이 플랫폼 버전이 하나의 자릿수로 표시될 경우는 앞자리는 생략합니다.

■ 네트워크 장비 버전 관리 절차

한화 비전 네트워크 장비는 플랫폼을 기반으로 제품 펌웨어가 개발되고 있습니다. 제품 펌웨어에서 개발된 기능은 플랫폼으로 재통합되어 신규 제품 개발을 위해 사용되는 순환 구조를 가지고 있습니다.



Hanwha Vision Co., Ltd.
13488 Hanwha Vision R&D Center,
6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL 070.7147.8771-8
FAX 031.8018.3715
www.HanwhaVision.com