보안 위협에 취약한 레거시 의료기기 사이버 보안 지침

방지호 (재)한국기계전기전자시험연구원 지능정보사업본부 본부장

1. 머리말

IMDRF/CYBER WG/N70:2023에서 정의한 용어정의에 따라, 레거시 의료기기는 지원 종료 이후 사이버 보안 위협에 취약한 의료기기라고 할 수 있다.

의료기기를 국내에서 시판하거나 해외에 수출하기 위해선 해당 국가의 의료기기 규제기관을 통해 인·허가를 받아야 한다. 예를 들어, 우리나라의 경우는 식품의약품안전처, 미국은 FDA(미국 식품의약국, Food and Drug Administration)에서 인·허가를 받는다.

최근 의료기기는 인·허가를 받기 위해 사이버 보안을 고려해 개발돼야 하며, 인·허가 이후 발생하는 취약점에 대응할 수 있는 관리체계를 구축해야 한다. 그러나, 제조사를 통한 지원이 종료된 레거시 의료기기는 사이버 보안 관리체계에서 고려하고 있지 않다.

이에 따라, 사이버 보안 관리에 취약한 레거시 의료기기에 대해, 사이버 보안 지침을 마련하는 것이 필요하다. 의료기기 전체 수명주기 단계 중 사이버 보안 위협에 취약한 레거시 의료기기에 대한 관점으로, 사이버 보안 주요 활동 지침을 제공하기 위한 표준을 소개한다.

2. '의료기기 시판 후 사이버 보안 취약점 대응 절차'와의 차이점

'의료기기 시판 후 사이버 보안 취약점 대응 절차(TTAK.KO-12.0381)'는 규제기관으로부터 허가·심사를 받은 의료기기 시판 후 발생하거나 발생할 수 있는, 사이버 보안 취약점 대응을 위한 절차를 제시하고 있다. 이에 비해, '보안위협에 취약한 레거시 의료기기 사이버 보안 지침'은 시판 후 의료기기 단종 및 서비스 지원 종료로 인해 사이버 보안에 대한 지원을 받을 수 없는, 레거시 의료기기에 대한 사이버 보안 지침을 제시하고 있다는 차이가 있다.

3. '보안 위협에 취약한 레거시 의료기기 사이버 보안 지침' 표준

3.1 표준 개발 목적

해당 지침의 목적은 시판 후 의료기기 단종 및 서비스 지원 종료로 인해 사이버 보안에 대한 지원을 받을 수 없는, 레거시 의료기기에 대한 사이버 보안 지침을 제시하는 것이다. 이를 통해, 의료기기 수명주기 전반에 걸쳐 사이버 보안에 대한 관리를 강화하

<표 1> 사이버 보안 관점의 의료기기 전체 수명주기

단계	개발	지원	제한적 지원	지원 종료
단계별 활동	• 사이버 보안을 고려해 설계 및 구현 • 제품 단종 및 지원 종료 계획 • 규제기관의 허가심사	• 제품 하드웨어 부품 및 소프트웨어 구성요소 업데이트 제공 * 보안 업데이트 포함 • 고객에게 단종 및 지원 종료 시점 전달 • 규제기관에 변경 정보 보고 등	• 제품 보안 업데이트만 제공 • 고객에게 지원 종료 시점 전달 • 규제기관에 변경정보 보고 등	• 제품에 대한 제조사의 보안지원 및 책임 종료
참고문서	• 안내서-0995-03 • TTAR-12.0040 • TTAK.KO-12.0372 • IMDRF/CYBER WG/N70FINAL:2023	• TTAK.KO-12.0381 • IMDRF/CYBER WG/N70FINAL:2023 • IMDRF/CYBER WG/N73FINAL:2023	• TTAK.KO-12.0381 • IMDRF/CYBER WG/N70FINAL:2023	• IMDRF/CYBER WG/N70FINAL:2023

고, 안전한 의료서비스를 제공할 수 있도록 지원한다.

3.2 표준 요약

레거시 의료기기 사이버 보안 지침은 소프트웨어를 포함하는 의료기기(펌웨어 및 프로그램 가능 논리 제어기(PLC)를 포함하는 의료기기 또는 소프트웨어 의료기기(SaMD))를 대상으로 한다. 국내의 경우, 사이버 보안 적용 대상은 유무선 통신을 사용하거나 통신 경로가 존재하는 의료기기다. 그러나, 해외의 경우 유무선 통신과 관계없이 사이버 보안을 적용하고 있다.

3.2.1 수명주기

소프트웨어 의료기기, 펌웨어 등을 포함한 의료기기 전체 수명주기는 <표 1>과 같이 개발, 지원, 제한적 지원, 지원 종료 단계로 구성되며, 제품 개발 제품의 허가·심사/단종(EOL)/지원 종료(EOS)에 따라 각 단계가 변경된다.

3.2.2 요구사항

3.2.2.1 개발 단계

의료기기 개발 단계에선 사이버 보안에 대한 위험관리를 수행해 사이버 보안 요구사항을 설계·구현해야 한다. 의료기기 개발 시 개발에 사용된 하드웨어 부품 또는 소프트웨어 구성요소에 대한 재료명세서(BOM)를 작성해야 한다.

의료기기 시판 전 의료기기 단종과 지원 종료에 대한 계획을 수립해 시판 시 고객에게 해당 정보를 알려주는 것이 필요하다. 해당 정보를 기반으로, 고객은 구매한 의료기기에 대한 업그레이드 또는 신규 제품 구매 등을 사전에 계획해 관련 예산을 확보할 수 있다.

의료기기 시판 전엔 관련 규제기관으로부터 허가심사를 받아야 하며, 이를 위해 사이버 보안과 관련된 내용을 기술문서 및 첨부자료에 반영해 제출해야 한다.

3.2.2.2 지원 단계

의료기기 지원 단계에서 제조사는 시판된 의료기

기의 하드웨어 부품 또는 소프트웨어 구성요소에 대한 업데이트를 고객에게 지원한다. 이때 업데이트는 보안 업데이트를 포함한다.

시판 중인 의료기기에서 발생되거나 발생할 가능성이 있는 사이버 보안 취약점에 대해서는 'TTAK.KO-12.0381(의료기기 시판 후 사이버 보안 취약점 대응 절차)'에 따라 처리한다.

의료기기 판매 시 제조사는 고객에게 소프트웨어 재료명세서(SBOM)를 전자문서 등의 형태로 제공해야 하며, 보안 업데이트를 포함한 소프트웨어 구성요소 업데이트가 발생하는 경우, 갱신된 소프트웨어 재료명세서를 제공해야 한다. 고객은 소프트웨어 재료명세서를 기반으로, 운용 중인 의료기기에 대한 취약점 파악 등 사이버 보안 관리를 수행할 수 있다.

3.2.2.3 제한적 지원 단계

의료기기 제한적 지원 단계는 시판 중인 의료기기의 단종 이후 단계다. 이는 신규 기능 추가·성능 개선과 같은 소프트웨어 지원을 제공하지 않고, 취약점에 대한 보안 업데이트만 제공한다.

의료기기 단종 시, 제조사는 관련 제품 구매 고객에게 단종 여부를 알려 고객이 제품 업그레이드, 대체 신규 제품 구매와 같이 적절한 대응을 할 수 있도록 한다. 또한, 지원 종료 시점 또는 예상 시점 정보를 제공한다.

고객은 지원 종료 단계 이전인 제한적 지원 단계에서 제품을 업그레이드하거나 대체 신규 제품을 구매해야 한다. 이를 위해, 관련 제조사에 업그레이드 또는 대체 제품에 대해 문의하고 견적을 요청해 구매를 진행하는 것이 필요하다. 제품 교체 전까지 고객은 소프트웨어 재료명세서를 기반으로 운용 중인 의료기기에 대한 사이버 보안 관리를 수행해야 하며, 제조사에서 제공하는 보안 업데이트 또는 권고사항을 적용해야 한다.

3.2.2.4 지원 종료 단계

의료기기 지원 종료 단계는 제품에 대한 보안 업데이트를 포함한 모든 지원을 제공하지 않는 상태이며, 시판된 의료기기에 대한 제조사의 모든 책임이 종료되는 단계다. 제조사는 제한된 서비스 지원이 종료된 의료기기 구매자 또는 운용 고객에게 지원 종료 단계에 도달됐음을 알리고, 제품 사용에 대한 모든 책임이 고객에게 있음을 전달한다.

고객은 지원 종료 단계 이전에 해당 의료기기를 교체하는 것이 필요하다. 그러나, 대체할 의료기기가 없거나, 관련 예산을 확보하지 못했거나, 대체할 의료기기가 없는 경우처럼 지원 종료 단계 이후에도 해당 의료기기를 계속 또는 일정 기간 동안 사용해야 하는 경우가 생길 수 있다.

지원 종료된 의료기기는 레거시 의료기기로서, 이는 제조사의 보안 업데이트 지원을 받을 수 없기 때문에 현재 사이버 보안 위협으로부터 적절히 보호될 수 없다. 이에 따라, 레거시 의료기기를 사용해야 하는 경우, 그 취약점이 외부에 노출되거나 악용되지 않도록 다음과 같은 보완 조치를 고려해 적용할 수 있다.

a) 침입차단 시스템, 침입방지 시스템 등과 같은 네트워크 보안 제품을 설치해 외부로부터의 임의 접근을 통제
b) 물리적으로 출입이 통제되는 구역 내에 의료기기를 설치·운영하고 허가된 사용자만 접근 허용
c) 의료기기 운영환경에 대한 모니터링
d) 의료기기에 대한 원격 접속 차단
e) 의료기기에 불필요한 기능 및 서비스(또는 포트) 비활성화
f) 의료기기를 네트워크에 연결하지 않도록 분리
g) USB처럼 인가되지 않은 외부 저장매체 사용 통제, 사용 전 악성코드 감염 여부 확인 등

4. 맺음말

'보안위협에 취약한 레거시 의료기기 사이버 보안 지침'은 대상 의료기기의 개발 단계, 지원 단계, 단종에 따른 제한적 지원 단계, 지원 종료 단계 등 전체 수명주기에 걸쳐, 의료기기 제조사와 고객이 취해야 할 사이버 보안 활동을 정의한 것이다. 또한, 지원 종료 이후 레거시 의료기기에 대해 고객이 취할 수 있는 사이버 보안 활동도 제시했다.

해당 지침을 통해 의료기기 제조사 및 수입업자, 의료기기 사용자 및 서비스 제공자들은 의료기기가 지원 종료 단계로 전환되기 전·후, 즉 레거시 의료기기로 전환되는 시기에 보안이 취약한 레거시 의료기기를 계속 사용할지 여부 등을 결정할 수 있다. 이번 지침이 레거시 의료기기를 안전하게 관리할 수 있는 사이버 보안 관리 지침으로 활용될 수 있기를 기대해 본다.

참고문헌

[1] IMDRF, IMDRF/CYBER WG/N60FINAL:2020, Principles and Practices for Medical Device Cybersecurity, IMDRF, 2020

[2] TTAK.KO-12.0353-Part1, 디지털 포렌식 조사를 위한 통합 정보 처리 규격 - 제1부: 개요 및 요구사항, TTA, 2019

[3] FDA, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, FDA, 2023

[4] TTAK.KO-12.0381, 의료기기 시판 후 사이버 보안 취약점 대응 절차, TTA, 2021

[5] IMDRF, IMDRF/CYBER WG/N70FINAL:2023, Principles and Practices for the Cybersecurity of Legacy Medical Devices, IMDRF, 2023

[6] TTAR-12.0040, 의료기기 사이버 보안 요구사항(기술보고서), TTA, 2019

[7] TTAK.KO-12.0372, 의료기기 정보보호 요구사항, TTA, 2021

[8] 안내서-0995-03, 의료기기의 사이버 보안 허가·심사 가이드라인(민원인 안내서), 식품의약품안전처, 2023

[9] IMDRF/CYBER WG/N73FINAL:2023, Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity, IMDRF, 2023

주요 용어 풀이

- **단종**(End of Life): 제조업체가 정의한 유효 수명을 경과한 이후에는 제품을 더 이상 판매하지 않으며, 해당 제품이 사용자에 대한 알림을 포함한 공식적인 단종 절차를 완료했을 때 시작되는 제품의 수명 주기 단계
- **레거시**(Legacy): 과거에 개발돼 현재에도 사용 중인 낡은 하드웨어나 소프트웨어
- **레거시 의료기기**(Legacy Medical Device): 사이버 보안 위협들로부터 적절히 보호될 수 없는 의료기기로, 의료기기 제조사로부터 보안패치에 대한 지원 종료된 의료기기를 지칭
- **소프트웨어 구성요소 목록**(Software Bill of Materials): 상용, 오픈 소스, 기성품, 맞춤형 소프트웨어 구성요소를 포함하되 이에 국한되지 않는 소프트웨어 구성요소 목록