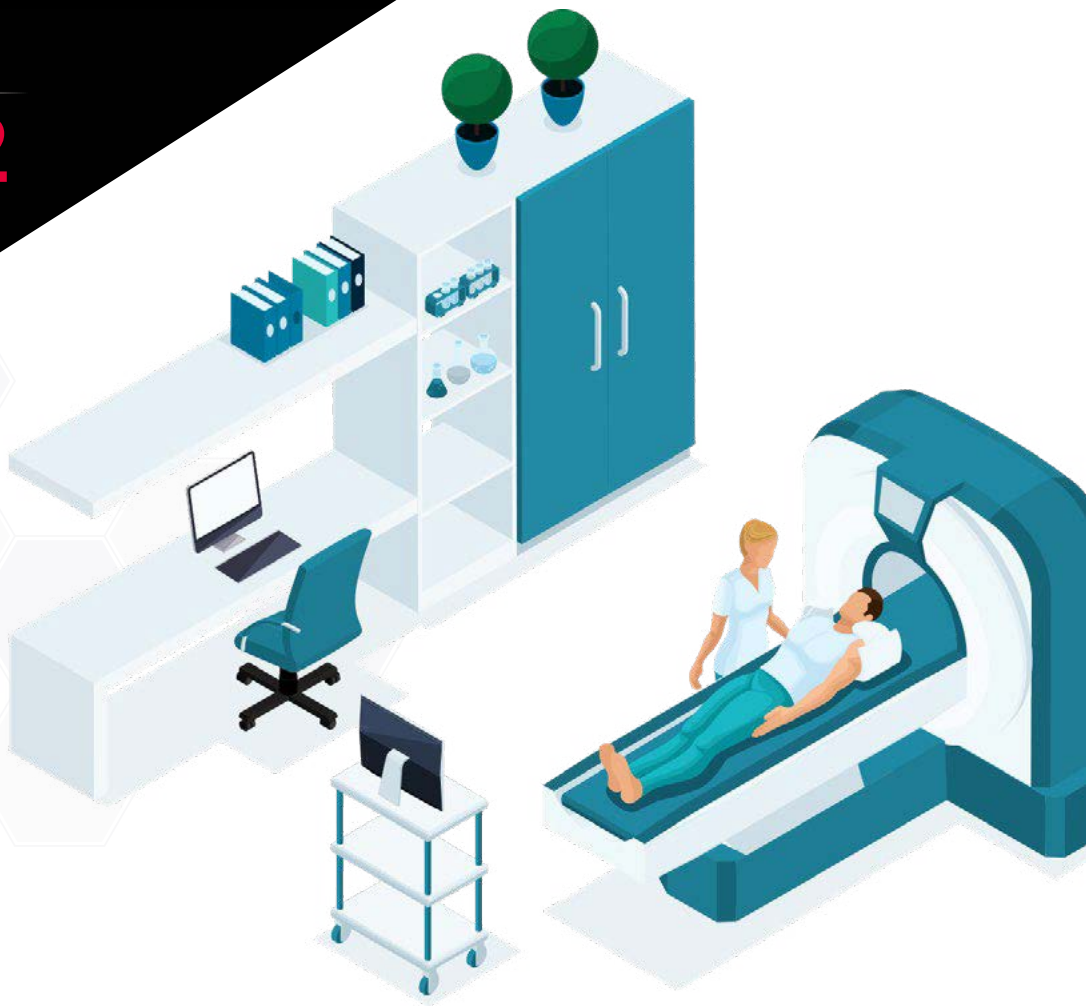
CLAROTY

TEAM82



CPS 보안 현황 보고서

헬스케어 2023

의료기기 보안과 전체 헬스케어 산업에 영향을 미치는
사이버보안 트렌드 및 이벤트에 대한 분석

요약

의료 산업에서는 의료 사이버보안과 개인정보보호를 동일시하는 분위기가 형성되어 있습니다. 지난 27년 간 미국 의료정보보호법(HIPAA)은 개인 환자 정보 보호에 초점을 맞추고 이를 기밀로 유지하기 위한 개인정보 보호 및 보안 규칙을 제정함으로써 이러한 접근법의 원동력이 되어왔습니다.

이 기간 동안, 특히 데이터 유출이 기승을 부리던 2000년대 초에는 이러한 전략이 의료 관련 사이버보안의 상징적 역할을 했습니다. 오늘날 커넥티드 의료기기의 운영 중단은 환자 치료와 삶의 질에 심각한 영향을 초래할 수 있습니다. 향후 온라인 환경에서 커넥티드 의료기기와 환자 시스템이 많아질수록 병원 운영을 마비시키려는 사이버공격도 늘어날 것으로 예상됩니다.

Team82의 첫 번째 "CPS 보안 현황 보고서: 헬스케어 2023"에서는 환자 안전에 영향을 주는 이러한 사이버보안 과제들을 살펴봅니다. 본 보고서에서는 의료 영상 시스템에서부터 주입 펌프까지 중요한 의료기기들의 광범위한 연결성을 확인하고 이러한 의료기기의 온라인 노출이 미치는 영향을 설명하고자 합니다. 조사 과정에서 여러 취약점과 구현 상의 약점을 발견할 수 있었으며, 이러한 사례들에서 이는 환자에게 부정적인 결과로 직결될 수 있습니다.

이번 조사를 통해 다음과 같은 사실을 확인할 수 있었습니다.

공격자가 악용할 수 있고 환자의 안전에 명확한 부정적 영향을 미치는, 알려진 취약점을 가진 의료기기가 아주 많습니다.

전통적으로 의료기기의 교체 주기는 사이버보안 문제가 아닌, 부품 고장 평균 시간에 따라 결정되어왔습니다.

이로 인해 보안에 취약한 의료기기가 계속 사용되고 있으며, 공격을 받을 경우 환자에게 부정적인 결과를 초래할 수 있습니다.

원격으로 제어 및 모니터링되는 의료기기가 확산되면서 의료기기 연결 네트워크와 같은 아키텍처 상의 약점과 그에 따른 위험이 발생하고 있습니다. 이로 인해 병원들이 외부 위협에 노출될 위험이 매우 높아지고 있습니다.

의료제공조직(HDO)이 사이버보안을 더 이상 사후적으로만 대응해서는 안 되는, 중요한 시점에 놓여 있음을 강조하고 싶습니다. 이제 사이버보안은 제조업체뿐만 아니라 의료제공조직에게도 핵심 비즈니스이자 전략적 고려사항이 되어야 하며, 이러한 점에서 의사결정자와 정책입안자가 이 보고서를 읽고 사이버보안에 대한 주요 이슈와 고려해야 할 위험에 대한 정보를 얻길 바랍니다.

주요 조사 결과

이 섹션의 데이터 포인트와 트렌드는 당사가 수행한 조사의 주요 결과를 보여줍니다. 구체적으로 의료 기기 및 구현이 공격에 어떻게 노출되는지 설명하고 우선적으로 위험을 완화해야 하는 영역을 보여줍니다.

의료기기에 존재하는 알려진 보안 취약점

미국 사이버보안 및 인프라 보안국(CISA)은 알려진 취약점(KEV) 목록을 꾸준히 업데이트하고 있습니다. 병원 네트워크에 존재하는 KEV가 특히 우려스러운데, 이러한 노출은 이를 침해하기 위해 작성된 익스플로잇이 있어 쉽게 침해될 수 있기 때문입니다. CISA가 추적한 KEV의 63%가 의료 네트워크에서 발견되며, 의료 영상 장비, 임상 IoT 기기, 수술 장비를 포함한 전체 의료기기 중에서 KEV가 한 가지 이상 존재하는 의료기기의 비율도 23%나 됩니다. 설상가상으로 사용자가 컴플라이언스 요구사항을 보장하고 제품이 위험에 대한 합리적인 보호 기능을 제공하는지 확인하려면 무려 360개의 의료기기 제조업체(MDM) 패치 인증 프로그램과 씨름해야만 합니다.

63%

CISA가 추적한 KEV 중 의료 네트워크에서 발견되는 KEV의 비율

360

사용자가 씨름해야 하는 의료기기 제조업체 패치 인증 프로그램 수

KEV란?

CISA는 공개적으로 알려진 공격에 사용된 소프트웨어 취약점 및 약점에 대한 데이터베이스를 운영합니다. KEV 목록은 익스플로잇이 공개적으로 알려진 소프트웨어 보안 취약점(CVE)으로 공개될 때마다 업데이트되며, 영향을 받은 벤더, 공개일, 해당 취약점에 대한 설명 및 완화 또는 치료에 대한 조언 등으로 구성됩니다. KEV 목록은 여기에서 확인할 수 있으며 보안 툴에 신속하게 통합할 수 있도록 기계 판독이 가능한 형식으로 제공됩니다.

병원 게스트 네트워크에서 발견되는 중요한 의료 자산

조사 결과, 수술에 사용되는 기기의 4%가 해당 병원의 게스트 네트워크를 통해서도 접속이 가능한 것으로 밝혀졌습니다. 게스트 네트워크는 병원 네트워크의 모든 영역 중에서 보안이 가장 취약하고 중요한 의료기기가 연결될 수 있는, 노출이 가장 심한 곳입니다.

의료기기 제조업체와 보안 패치 문제

의료기기 제조업체(MDM)는 윈도우나 리눅스 운영체제와 같이 패치와 업데이트가 주기적으로 이루어지는 플랫폼에서 개발을 하지만 이러한 기능이 의료기기에까지 구축되는 것은 아닙니다. 대신 취약점 패치는 이미 높은 비용을 지불하고 있는 기술 지원 계약의 추가 서비스 형태로 제공되는 경우가 많다고 당사가 대화를 나눠본 의료제공조직들은 전합니다.

또한 많은 의료기기 제조업체들은 지원되지 않는 운영체제를 기반으로 실행되는 기기에 대한 지원 계약을 제공합니다. 이로 인해 의료제공조직들은 취약점이나 구현 상의 약점을 완화하기 위해 보완 통제에 의존해야 합니다.

한편 의료기기 제조업체들은 미 식품의약국(FDA)의 의료기기 인증 절차가 너무 오래 걸려서 FDA 인증 기능이 침해될 우려가 있기 때문에 완전한 보안 테스트에 투자하기를 꺼리게 된다고 주장합니다.

환자의 안전을 위협하는 구형 시스템

분석 결과, 커넥티드 의료기기의 14%가 지원되지 않거나 기술 지원이 종료된 운영체제를 사용하고 있는 것으로 나타났습니다. 지원되지 않는 기기 중 32%는 진단 및 처방 치료에 중요한 엑스레이나 MRI와 같은 의료 영상 기기입니다. 또한 병원에 수백 대씩 있는 주입 펌프나 기타 환자 기기와 달리 의료 영상 기기는 많지 않기 때문에 한 대 이상이 작동하지 않을 경우 심각한 가용성 문제가 발생할 수 있습니다.

4%

병원의 게스트 네트워크를 통해 접속이 가능한 수술 기기의 비율

14%

지원되지 않거나 기술 지원이 종료된 운영체제를 사용하는 커넥티드 의료기기의 비율

임상 IoT 기기(23%)와 병원 정보 시스템(20%) 역시 지원되지 않거나 기술 지원이 종료된 운영체제를 사용하는 기기입니다. 이렇게 지원되지 않는 운영체제의 상당수가 윈도우이지만 이 외에도 리눅스 시스템에서부터 모바일 운영체제, 심지어 구형 SUN 솔라리스 및 SUN 운영체제에 이르기까지 다양한 미지원 운영체제가 사용되고 있습니다.

이러한 조사 결과는 레거시 운영체제를 사용하는 시스템에 벤더에서 패치 제공을 중단한 심각한 취약점이 있을 수 있고 이로 인해 의료기기가 심각한 위협에 노출될 수 있음을 시사합니다.

지원되지 않는 운영체제를 사용하는 수술 기기

앞선 조사 결과에 덧붙이자면, 고장이 발생할 경우 환자의 안전을 위협할 수 있는 수술 기기 중 지원되지 않거나 기술 지원이 종료된 운영체제를 사용하는 기기가 7%나 됩니다. 이러한 수술 기기에는 로봇 수술 시스템, 제세동기 및 게이트웨이, 인공호흡기, 마취 및 모니터링 시스템이 포함됩니다.

의료제공조직에서 취약점이 만연할 것으로 예상되는 의료기기

환자 기기의 11%와 고장 시 환자 치료에 부정적인 영향을 미칠 수 있는 중요 장비인 수술 기기의 10%가 EPSS 스코어가 높은 취약점을 가지고 있습니다. 이 자산들은 현재로서는 알려진 취약점이 없지만, EPSS 스코어가 높다는 것은 향후 취약점이 발견될 가능성이 그만큼 높다는 것을 시사합니다.

CVE 개수 기준 취약 의료기기

의료 영상 워크스테이션과 의료영상 저장 전송 시스템(PACS) 서버는 공개된 CVE가 각각 18,000건과 12,000건으로 압도적으로 많은 2대 의료기기 범주입니다. 진단 워크스테이션, 수술 안전 기기, EEG 장비도 상위 10위 안에 포함됩니다. 이러한 기기들은 대부분이 레거시 윈도우 운영체제를 사용하기 때문에 패치뿐만 아니라 신원 확인과 세그먼테이션에도 문제가 있습니다.

7%

고장이 발생할 경우 환자의 안전을 위협할 수 있는 수술 기기 중 지원되지 않거나 기술 지원이 종료된 운영체제를 사용하는 기기의 비율

익스플로잇 예측 스코어링 시스템(EPSS):

사고대응 및 보안팀 포럼(FIRST)이 개발한 **EPSS 스코어**(0~100점)는 어떤 소프트웨어 취약점이 실제 환경에서 악용될 가능성을 보여주는 지표입니다. EPSS 스코어는 CVE 및 실제 익스플로잇에 대한 최신 위협 정보를 기반으로 산정됩니다.