TREND REVIEW

IoT THREAT

OWASP 선정 IoT 취약점 Top 10

IoT 시스템 관리, 가장 큰 문제와 취약점은 무엇일까?

사물인터넷(Internet of Things, 이하 IoT)은 가전에서부터 자동차, 물류, 유통, 헬스케어에 이르기까지 다양한 분야에서 활용되고 있다. 글로벌 IT기업 시스코(Cisco)는 2022년까지 전 세계의 네트워킹 기기가 약 285억개에 달할 것으로 보았으며 그 중 절반 이상이 IoT라고 전망하기도 했다.

한편 IoT 시장이 급증함에 따라 IoT 취약점에 대한 보안 문제가 새로운 과제로 떠올랐다. IoT 디바이스가 해커들의 주요 공격 목표로 부상할 가능성이 높아졌으나 IoT에 적용되는 보안 표준은 다소 느슨하거나 제대로 지켜지지 않고 있기 때문이다.

이에 OWASP(The Open Web Application Security Project)가 발표한 IoT의 10대 취약점을 소개한다.

OWASP의 가이드는 IoT 보안에 대한 이해를 높이고 사용자가 IoT 기술을 구축 · 배포 · 평가 시 도움을 줄 수 있다. 특히 그 동안 발표된 IoT 보안 가이드가 각 대상과 업계, 분야에 정교하게 맞추어져 있는 것과는 달리, 제조업체, 기업, 소비자를 포괄하는 관점에서 단일화되어 있어 일반 사용자와 관련 업체가 주목할 만하다. 지금부터 OWASP가 발표한 IoT의 10대 취약점을 자세히 알아보자.

IoT의 10대 취약점

1. 쉬운 암호, 추측 가능한 암호 또는 하드코딩된 암호

펌웨어 또는 클라이언트 소프트웨어의 백도어를 포함하여 배포된 시스템에 무단 액세스 권한을 부여하는 공개적인 인증 정보 혹은 변경할 수 없는 인증 정보를 사용하는 경우.

2. 안전하지 않은 네트워크 서비스

디바이스 자체에서 실행되는 불필요하고 안전하지 않은 네트워크 서비스. 특히 인터넷에 노출되어 기밀성, 무결성/신뢰성, 또는 정보 가용성을 훼손하거나 무단 원격 제어를 허용하는 서비스의 경우.

3. 안전하지 않은 에코시스템 인터페이스

디바이스 또는 관련 구성 요소를 손상시킬 수 있는 외부 에코시스템의 불안한 웹, 백엔드 API, 클라우드 또는 모바일 인터페이스. 일반적인 문제로는 인증/승인 부재, 암호화 부재 또는 취약한 암호화, 취약한 입력 및 출력 필터링 등이 있다.

4. 보안 업데이트 메커니즘 부재

디바이스를 안전하게 업데이트할 수 있는 기능이 없는 경우. 디바이스에 대한 펌웨어 검증 부재, 안전한 전달 부재(전송 중 암호화되지 않음), 롤백 방지 메커니즘 부재, 업데이트로 인한 보안 변경 사항 알림 부재 등의 문제가 발생할 수 있다.

5. 안전하지 않거나 오래된 구성 요소 사용

디바이스를 손상시킬 수 있는 불필요하고 안전하지 않은 소프트웨어 구성요소/라이브러리가 사용되는 경우. 운영체제 플랫폼의 안전하지 않은 사용자 정의와 손상된 공급망의 타사 소프트웨어 또는 하드웨어 구성 요소 사용이 포함된다.

6. 불충분한 개인정보보호

디바이스 및 에코시스템에 저장된 사용자의 개인정보가 불안정하게, 부적절하게, 또는 허가 없이 사용되는 경우.

7. 안전하지 않은 데이터 전송 및 저장

보관, 전송 또는 처리 중을 포함한 에코시스템 내 어느 단계에서나 중요한 데이터에 대한 암호화 또는 액세스 제어가 이뤄지지 않는 경우.

8. 디바이스 관리 부재

자산 관리, 업데이트 관리, 안전한 폐기, 시스템 모니터링 및 대응 기능을 포함하여 운영 환경에 구축된 디바이스에 대한 보안 지원이 부족한 경우.

9. 안전하지 않은 기본 설정

안전하지 않은 기본 설정 상태로 출하되는 디바이스 또는 시스템은 운영자가 구성을 수정하지 못하도록 제한하여 시스템을 보다 안전하게 만들 수 있는 기능이 부재한 경우.

10. 물리적 하드닝(Hardening) 부족

물리적 하드닝이 부족하기 때문에 잠재적인 공격자가 향후 원격 공격에 활용할 민감한 정보를 얻거나 디바이스를 내부에서 제어할 수 있도록 하는 경우.

OWASP는 “IoT 전망 보고서를 더욱 확대할 계획”이라고 밝혔다. 2년마다 발행하고 있는 목록을 개선하기 위해 추가 피드백을 통해 현재 산업이 직면하고 있는 문제에 대한 최신 정보를 제공할 계획이다. 뿐만 아니라 ICS/SCADA 등 IoT의 다른 측면으로 프로젝트를 확장하는 것을 논의 중이다. 여러가지 예시와 함께 악용 사례, 유즈케이스 등을 추가하여 논의된 각 개념을 공고히 할 것이다. 또한 사용자들에게 무엇을 피해야 하는지 뿐만 아니라 안전하게 작업을 수행하려면 무엇을 지켜야 하는지에 대해서 기준도 정해준다는 계획이다.