소비자 IoT 보안을 위한 실무 지침

제목

소비자 IoT 보안을 위한 실무 지침

날짜

2018년 10월

내용 요약

가정에서 인터넷에 연결하는 장치가 점점 늘어나면서 기존에는 인터넷에 연결하지 않고 사용하던 제품이나 기기가 이제 '사물 인터넷(IoT)'의 일부가 되고 있습니다.

IoT는 가정에서 기술이 점점 더 일상화되고 있음을 나타내며 생활을 보다 편안하고 즐겁게 만들어 주는 역할을 합니다. 온라인 장치와 서비스에서 점점 더 많은 개인 정보를 관리하고 있으므로 이러한 제품의 사이버 보안은 이제 주택의 물리적 보안 못지 않게 중요합니다.

이 실무 지침의 목적은 제품이 처음부터 안전하게 설계되고 디지털 환경에서 보다 쉽게 보안을 유지할 수 있도록 지침을 제공하여 소비자 IoT 개발, 제조 및 소매에 참여하는 모든 당사자를 지원하는 것입니다.

이 실무 지침은 IoT 보안의 모범 사례로 널리 알려진 결과 중심의 지침 13개를 제공합니다. 이러한 지침은 DCMS(Digital, Culture, Media and Sport) 부서가 NCSC(National Cyber Security Centre)와 함께 개발했으며 산업, 소비자 협회 및 학계가 협력하고 있습니다. 이 지침은 Secure by Design(계획된 보안) 보고서에 포함되어 2018년 3월 초안이 처음 발표되었습니다.[1]

소개

IoT(사물 인터넷)는 사람들에게 많은 혜택을 제공하지만 현재 출시된 장치 중 상당수가 기본적인 보안 대책을 갖추지 못한 것으로 확인되었습니다. 사용자가 커넥티드 기술을 안전하게 활용할 수 있도록 온라인 활동을 보호할 수 있는 적절한 보안 및 개인 정보 보호 대책을 갖춰야 합니다.

---

[1] DCMS, 2018, 'Secure by Design: Improving the cyber security of consumer Internet of Things: Report(계획된 보안: 소비자 사물 인터넷의 사이버 보안 강화: 보고서)', https://www.gov.uk/government/publications/secure-by-design

이 실무 지침은 IoT 제조업체 및 기타 업계 이해관계자들에게 소비자 IoT 제품 및 관련 서비스의 보안을 강화하기 위한 실질적인 방법을 제시합니다. 13가지 지침을 이행하면 소비자의 개인 정보 보호와 안전을 보호하는 동시에 제품을 보다 안전하게 사용하는 데 도움이 됩니다. 또한 보안이 취약한 IoT 장치 및 서비스에서 발생하는 DDoS(Distributed Denial Of Service) 공격도 방지할 수 있습니다.

이 지침은 IoT 보안에 있어 널리 알려진 모범 사례를 통합하여 제공합니다. 관행에 치우치지 않고 결과에 초점을 맞추므로 조직에 맞게 이 지침을 적용하여 자사 제품에 적합한 보안 솔루션을 혁신하고 구현할 수 있습니다.

이 실무 지침만으로 모든 보안 문제를 해결할 수 있는 것은 아닙니다. 사고방식을 보안 중심으로 전환하고 안전한 개발 수명 주기에 투자해야만 조직이 안전한 IoT를 구축하는 데 성공할 수 있습니다. 제품 및 서비스는 제품 개발부터 전체 수명 주기 동안 보안을 염두에 두고 설계되어야 합니다. 또한 조직은 제품 및 서비스와 관련된 사이버 보안 위험을 정기적으로 평가하고 이러한 문제를 해결하기 위한 적절한 조치를 취할 수 있어야 합니다.

IoT 제품의 공급망은 복잡하고 국제적일 수 있으며 여러 구성 요소 제조업체와 서비스 공급자가 관련된 경우가 많습니다. 이 지침의 목적은 공급망 전체에서 긍정적인 보안 변화를 시작하고 촉진하는 것입니다.

많은 업계 단체와 국제 포럼에서 IoT에 대한 보안 권고사항과 표준을 개발하고 있습니다.[2] 이 실무 지침은 이러한 개발 노력과 발표된 사이버 보안 표준을 보완하고 지원하기 위해 만들었습니다. 소비자 IoT에 관련된 향후 보증과 신뢰마크 체계가 이 지침에 부합할 것이라는 희망을 바탕으로 업계와 함께 직접 만든 것입니다.

실무 지침을 이행하면 조직이 관련 데이터 보호법을 준수하는 데 도움이 될 수 있습니다. 예를 들어 EU GDPR(General Data Protection Regulation, 일반 개인 정보 보호법)을 따라 개인 정보를 안전하게 처리해야 합니다.[3]

이행

[2] PETRAS, 2018, 'Summary literature review of industry recommendations and international developments on IoT security(IoT 보안에 대한 업계 권고사항 및 국제 개발 요약 문헌 검토)', https://www.gov.uk/government/publications/secure-by-design

[3] GDPR 5(1)(f)항은 개인 정보의 '무결성 및 기밀성'에 관련된 내용입니다.

실무 지침은 각 지침을 주요 업계 표준, 권고사항 및 안내에 연결하는 매핑 문서로 지원됩니다.[4] 이 문서는 지침의 13개 지침에 대한 추가적인 상황 정보를 제공하며 업계에서 이를 이행하는 데 도움이 됩니다. 이 문서에서는 광범위한 글로벌 조직에서 수행하는 IoT 보안에 대한 지침 및 업무 간의 관계도 설명합니다.

우선 순위 및 구조

기본 암호, 취약성 공개 및 보안 업데이트에 대한 조치가 단기간에 가장 큰 보안 이점을 제공하기 때문에 처음 세 가지 지침이 우선 순위가 높습니다.

근거 텍스트는 각 지침에 대한 이론적 근거를 설명하고 각 가이드라인에 대한 세부 정보를 추가합니다. 문서 끝에 있는 추가 설명은 자주 묻는 질문에 대한 답변입니다.

대상

각 지침에 주로 이행을 책임지는 이해관계자 대상을 표시합니다. 이해관계자는 다음과 같이 정의됩니다.

장치 제조업체	인터넷에 연결된 최종 조립 제품을 만드는 기업입니다. 최종 제품에는 여러 다른 제조업체의 제품이 포함될 수 있습니다.
IoT 서비스 공급자	IoT 솔루션의 일부로 패키징된 네트워크, 클라우드 스토리지 및 데이터 전송과 같은 서비스를 제공하는 회사입니다. 인터넷에 연결된 장치는 서비스의 일부로 제공될 수 있습니다.
모바일 애플리케이션 개발자	모바일 장치에서 실행되는 애플리케이션을 개발하고 제공하는 기업입니다. 이러한 애플리케이션은 IoT 솔루션의 일부로 장치와 상호 작용하는 방식으로 제공되는 경우가 많습니다.
판매업체	인터넷에 연결된 제품 및 관련 서비스를 소비자에게 판매합니다.

용어

[4] DCMS, 2018, 'Mapping of IoT Security Recommendations, Guidance and Standards to the Code of Practice for Consumer IoT Security(소비자 IoT 보안을 위한 실무 지침에 대한 IoT 보안 권고사항, 안내 및 표준 매핑)', Https://www.gov.uk/government/publications/secure-by-design

'Security-sensitive data(보안에 민감한 데이터)'라는 용어는 GDPR에 정의된 특수 범주 데이터(공식적으로 'sensitive personal data(중요한 개인 정보)')와 같은 다른 유형의 중요 데이터와 구별하기 종류의 중요 데이터를 구별하기 위한 것입니다. 보안에 민감한 데이터에는 암호화 초기화 벡터와 같은 데이터가 포함될 수 있습니다.

'consumer(소비자)'라는 용어는 일관성을 위해 전반적으로 사용되며, 일반적으로 소비자는 IoT 제품과 서비스의 최종 사용자로 간주됩니다.

적용 범위

이 실무 지침은 인터넷 및/또는 홈 네트워크와 관련 서비스에 연결된 소비자 IoT 제품에 적용됩니다. 몇 가지 예를 들면 다음과 같습니다:

- 연결된 어린이용 장난감과 아기 모니터
- 화재 감지기 및 도어 잠금 장치 등 연결된 안전 관련 제품
- 스마트 카메라, TV 및 스피커
- 웨어러블 헬스 트래커
- 연결된 홈 자동화 및 경보 시스템
- 연결된 가전(예: 세탁기, 냉장고)
- 스마트 홈 비서

관련 서비스는 모바일 애플리케이션, 클라우드 컴퓨팅/스토리지 및 메시징과 같은 서비스에 대한 타사 애플리케이션 프로그래밍 인터페이스(API)와 같은 IoT 장치에 연결된 디지털 서비스로 간주됩니다.

검토

DCMS(Digital, Culture, Media and Sport) 부서에서는 정기적으로 이 지침을 검토하고 적어도 2년마다 업데이트를 게시합니다. 최신 정보를 받으려면 securebydesign@culture.gov.uk에 문의하십시오.

지침

1) 기본 암호 없음

모든 IoT 장치 암호는 고유해야 하며 일반적인 공장 출하 시 기본값으로 재설정할 수 없어야 합니다.

많은 IoT 장치가 소비자가 변경할 것으로 예상되는 일반적인 기본 사용자 이름 및 암호(예: "admin, admin")로 설정되어 판매되고 있습니다. IoT에서 많은 보안 문제를 발생시킨 원인인 이러한 관행은 없애야 합니다. 암호 및 기타 인증 방법에 대한 모범 사례를 따라야 합니다.[5]

주요 대상: 장치 제조업체

2) 취약성 공개 정책 이행

인터넷에 연결된 장치 및 서비스를 제공하는 모든 회사는 보안 연구원이나 다른 사용자가 문제를 보고할 수 있도록 취약성 공개 정책의 일부로 담당자 연락처를 제공해야 합니다. 공개된 취약성은 적시에 조치를 취해야 합니다.

회사에서 보안 취약성을 알고 있으면 대응할 수 있습니다. 또한 회사는 제품 보안 수명 주기의 일부로 자사 제품 및 서비스의 보안 취약성을 지속적으로 모니터링하고 파악한 후 해결해야 합니다. 우선 영향을 받는 이해관계자에게 취약성을 직접 보고해야 합니다. 이렇게 할 수 없는 경우 취약성을 국가 기관에 보고할 수 있습니다.[6] 여러 상황에서 취할 수 있는 다양한 접근 방법에 대한 자세한 내용은 추가 설명을 참고할 수 있습니다. 또한 회사는 관할 산업 기관과 정보를 공유하는 것이 좋습니다.[7]

주요 대상: 장치 제조업체, IoT 서비스 공급자 및 모바일 애플리케이션 개발자

3) 소프트웨어 최신 업데이트 유지

---

[5] 안내를 보려면 다음을 참조하십시오. NCSC, 2016, 'Password Guidance: Simplifying Your Approach(암호 지침: 접근 방식의 간소화)', https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach 참고 항목: NIST, 2017, 'NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management(NIST 특별 발행 800-63B: 디지털 ID 가이드라인 - 인증 및 수명 주기 관리)', https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

[6] 영국에서는 취약성 보고서를 https://www.ncsc.gov.uk/contact로 보낼 수 있습니다.

[7] 관할 산업 기관에는 GSMA와 IoT Security Foundation이 포함됩니다. IoT Security Foundation에서 이 취약성 공개에 대한 ISO/IEC 29147 표준을 참조하는 Guidance on Coordinated Vulnerability Disclosure(협정 취약성 공개 안내)를 이용할 수 있습니다. GSMA 업계 수준의 Coordinated Vulnerability Disclosure(협정 취약성 공개) 프로그램은 https://www.gsma.com/cvd에 있습니다.

인터넷에 연결된 장치의 소프트웨어 구성 요소는 안전하게 업데이트할 수 있어야 합니다. 업데이트는 시기 적절해야 하며 장치의 기능에 영향을 주지 않아야 합니다. 수명 종료 정책은 엔드 포인트 장치에 대해 게시되어 장치가 소프트웨어 업데이트를 수신하는 최소 시간 및 지원 기간에 대한 이유를 명시적으로 나타내야 합니다. 각 업데이트에 대한 필요성을 소비자에게 분명히 설명해야 하며, 업데이트를 쉽게 실행할 수 있어야 합니다. 물리적으로 업데이트할 수 없는 제한된 장치의 경우, 해당 제품은 분리 가능하고 교체 가능해야 합니다.

또한 보안 패치의 출처도 보증하고 보안 채널을 통해 전달해야 합니다. 장치의 기본 기능은 가능하면 업데이트 중에도 계속 작동해야 합니다. 예를 들어, 시계는 계속 작동하며 시간을 알려주고, 실내 온도조절장치가 계속 작동하고 잠금 장치는 잠금 해제 및 잠금을 계속해야 합니다. 이는 주로 설계 고려 사항이지만 적절히 고려하지 않거나 관리하지 않을 경우 일부 유형의 장치 및 시스템에서 심각한 보안 문제가 발생할 수 있습니다.

장치 판매 후에 소프트웨어 업데이트를 제공해야 하며 적절한 기간 동안 장치에 푸시해야 합니다. 이 소프트웨어 업데이트 지원 기간은 제품 구입 시 소비자에게 명확하게 설명해야 합니다. 판매업체 및/또는 제조업체는 소비자에게 업데이트가 필요함을 알려야 합니다. 소프트웨어 업데이트를 사용할 수 없는 제한된 장치의 경우, 교체 지원 조건 및 기간이 명확해야 합니다.

주요 대상: 장치 제조업체, IoT 서비스 공급자 및 모바일 애플리케이션 개발자

4) 자격 증명 및 보안에 민감한 데이터를 안전하게 저장

서비스 및 장치에 모든 자격 증명을 안전하게 저장해야 합니다. 장치 소프트웨어에서 하드 코딩된 자격 증명은 허용되지 않습니다.

장치 및 애플리케이션의 리버스 엔지니어링으로 소프트웨어에서 하드 코딩된 사용자 이름 및 암호와 같은 자격 증명을 쉽게 검색할 수 있습니다. 또한 이 하드 코딩된 정보를 숨기거나 암호화하는 데 사용되는 간단한 난독화 방법을 쉽게 해독할 수 있습니다. 안전하게 저장해야 하는 보안에 민감한 데이터에는 암호화 키, 장치 식별자, 초기화 벡터 등이 있습니다. 안전하고 신뢰할 수 있는 스토리지 메커니즘은 신뢰된 실행 환경 및 관련된 신뢰할 수 있는 안전한 스토리지에서 제공하는 메커니즘과 같이 사용되어야 합니다.

주요 대상: 장치 제조업체, IoT 서비스 공급자, 모바일 애플리케이션 개발자

5) 안전한 통신

모든 원격 관리 및 제어를 비롯한 보안에 민감한 데이터는 전송 중에 암호화되고 기술 및 사용 속성에 적합해야 합니다. 모든 키를 안전하게 관리해야 합니다.

동종 업계에서 검토된 개방된 인터넷 표준을 사용하는 것이 좋습니다.

주요 대상: 장치 제조업체, IoT 서비스 공급자, 모바일 애플리케이션 개발자

6) 공격에 대한 노출 최소화

모든 장치 및 서비스가 최소 권한 원칙으로 작동해야 합니다. 사용되지 않는 포트는 닫혀 있어야 하며, 필요한 경우에만 하드웨어 액세스를 허용해야 합니다. 사용되지 않는 서비스는 제공하지 않고 서비스가 작동하는 데 필요한 기능으로 코드를 최소화해야 합니다. 소프트웨어는 보안 및 기능을 모두 고려하여 적절한 권한으로 실행해야 합니다.

최소 권한 원칙은 다양한 적용 분야에서와 마찬가지로 IoT에 적용할 수 있는 우수한 보안 엔지니어링의 기반이 됩니다.

주요 대상: 장치 제조업체, IoT 서비스 공급자

7) 소프트웨어 무결성 보장

보안 부팅 메커니즘을 사용하여 IoT 장치의 소프트웨어를 검증해야 합니다. 무단 변경이 감지될 경우 이 장치는 소비자 관리자에게 문제를 알려야 하며 경고 기능을 수행하는 데 필요한 것보다 더 넓은 네트워크에 연결해서는 안 됩니다.

이러한 상황에서 원격으로 복구하는 기능은 정상 작동이 확인된 버전을 로컬로 저장하는 것과 같은 알려진 정상 상태를 사용하여 장치를 안전하게 복구하고 업데이트할 수 있습니다. 이렇게 하면 서비스 거부 및 비용이 많이 드는 리콜 또는 유지 관리 방문을 방지할 수 있으며 업데이트 또는 기타 네트워크 통신 메커니즘을 파괴하는 공격자가 장치를 제어할 잠재적인 위험을 관리할 수 있습니다.

주요 대상: 장치 제조업체

8) 개인 정보 보호 보장

장치 및 또는 서비스가 개인 정보를 처리하는 경우 GDPR(General Data Protection Regulation, 일반 개인 정보 보호법) 과 Data Protection Act 2018(데이터 보호법2018) 과 같은 관련 데이터 보호법에 따라 개인 정보를 보호해야 합니다. 장치 제조업체 및 IoT 서비스 공급자는 소비자에게 각 장치 및 서비스에 대해 개인 정보를 누가 어떤

목적으로 어떻게 사용하는지에 대한 정보를 명확하고 투명하게 제공해야 합니다. 또한 이는 관련될 수 있는 제3 자(광고주 포함)에게도 적용됩니다. 개인 정보가 소비자의 동의에 따라 처리되는 경우, 이는 타당하고 합법적으로 확보되어야 하며 소비자들은 언제든지 동의를 철회할 수 있어야 합니다.

이 지침은 다음을 보장합니다:
i) IoT 제조업체, 서비스 공급자 및 애플리케이션 개발자는 제품 및 서비스를 개발 및 제공할 때 데이터 보호 의무를 준수해야 합니다.
ii) 개인 정보는 데이터 보호법에 따라 처리됩니다.
iii) 사용자는 제품의 데이터 처리 작업이 일관되고 지정된 대로 작동하고 있는지 확인할 수 있습니다.
iv) 사용자에게 장치 및 서비스 기능을 적절하게 구성하여 개인 정보 보호를 유지할 수 있는 수단을 제공합니다.

주요 대상: 장치 제조업체, IoT 서비스 공급자, 모바일 애플리케이션 개발자, 판매업체

9) 운영 중단 시 시스템 복원

복원 기능은 데이터 네트워크 및 전원 중단의 가능성을 고려하여 사용에 필요하거나 다른 사용 시스템에 필요한 IoT 장치 및 서비스에 구축되어야 합니다. 합리적으로 가능한 한 IoT 서비스는 네트워크 연결이 끊어진 경우에도 작동 및 로컬 기능을 유지해야 하며 정전에서 복구하는 경우에는 정상적으로 복구되어야 합니다. 장치는 대규모로 재연결하는 대신 합리적인 상태에서 질서 정연하게 네트워크에 복귀할 수 있어야 합니다.

소비자는 안전에 관련이 있거나 생명에 영향을 미칠 수 있는 더욱 중요한 사용 사례에서 IoT 시스템과 장치에 의존하고 있습니다. 네트워크 연결이 끊어질 경우 로컬에서 서비스를 계속 실행하는 것은 복원력을 높이기 위해 취할 수 있는 조치 중 하나입니다. 다른 조치로는 서비스에 대한 이중화 구축 및 DDoS 공격에 대한 완화 요소가 포함될 수 있습니다. 필요한 복원 수준은 사용에 맞게 적절하게 결정해야 하지만 예상보다 더 큰 영향을 미칠 수 있으므로 시스템, 서비스 또는 장치에 의존할 수 있는 다른 사용자를 고려해야 합니다.

주요 대상: 장치 제조업체, IoT 서비스 공급자

10) 시스템 원격 측정 데이터 모니터링

IoT 장치 및 서비스에서 사용 및 측정 데이터와 같은 원격 측정 데이터를 수집하는 경우 보안 이상 여부를 모니터링해야 합니다.

로그 데이터를 비롯한 원격 측정 모니터링 기능은 보안 평가에 유용하며 비정상적인 상황을 조기에 식별하고 해결하여 보안 위험을 최소화하고 문제를 신속하게 해결할 수 있습니다. 단, 지침 8에 따라 개인 정보 처리는 최소한으로 유지되어야 하며 소비자에게 수집되는 데이터와 수집 이유에 대한 정보를 제공해야 합니다.

주요 대상: IoT 서비스 공급자

11) 소비자가 개인 정보를 쉽게 삭제할 수 있도록 지원

장치와 서비스는 소유권이 이전될 때 소비자가 개인 정보를 삭제하고자 할 때 및 또는 소비자가 장치를 폐기하고자 할 경우 개인 정보를 쉽게 삭제할 수 있도록 구성되어야 합니다. 소비자에게 개인 정보를 삭제하는 방법에 대한 명확한 지침을 제공해야 합니다.

IoT 장치는 소유권을 변경할 수 있으며 결국 재활용되거나 폐기됩니다. 소비자에게 서비스, 장치 및 애플리케이션에서 개인 정보를 제어하고 제거할 수 있는 방법을 제공할 수 있습니다.

주요 대상: 장치 제조업체, IoT 서비스 공급자, 모바일 애플리케이션 개발자

12) 쉬운 장치 설치 및 유지 관리

IoT 장치의 설치 및 유지 관리 단계를 최소화하고 보안 모범 사례를 따라야 합니다. 또한 소비자에게 장치를 안전하게 설정하는 방법에 대한 지침을 제공해야 합니다.

소비자가 혼동하거나 잘못 구성하여 발생하는 보안 문제는 UI(사용자 인터페이스)의 복잡성과 잘못된 설계를 적절하게 해결하면 줄이거나 때로는 완전히 없앨 수도 있습니다. 장치를 안전하게 구성하는 방법을 명확하게 안내하는 것으로도 위협에 대한 노출을 줄일 수 있습니다.

주요 대상: 장치 제조업체, IoT 서비스 공급자, 모바일 애플리케이션 개발자

13) 입력 데이터의 유효성 검사

사용자 인터페이스를 통한 데이터 입력과API(애플리케이션 프로그래밍 인터페이스) 를 통해 또는 서비스와 장치의 네트워크 간에 전송된 데이터는 유효성을 검사해야 합니다.

잘못된 형식의 데이터 또는 다른 유형의 인터페이스를 통해 전송된 코드로 인해 시스템에 문제가 발생할 수 있습니다. 공격자는 데이터의 유효성을 검사하지 않아 발생할 수 있는 허점과 약점을 악용하기 위해 자동화된 도구를 사용하는 경우가 종종 있습니다. 예를 들어 다음과 같은 데이터가 포함되지만 이에 국한되지는 않습니다.

i) 예상되지 않은 데이터 유형(예: 사용자가 입력한 텍스트가 아닌 실행 코드)

ii) 범위를 벗어나는 데이터(예: 센서 한계를 벗어나는 온도 값)

주요 대상: 장치 제조업체, IoT 서비스 공급자, 모바일 애플리케이션 개발자

추가 설명

기본 암호 없음에 대한 지침1: 암호에 대한 의존도를 없애고 사용자 및 시스템을 인증하는 대체 방법을 제공하기 위해 많은 노력을 기울였지만 일부 IoT 제품은 UI(사용자 인터페이스)에서 네트워크 프로토콜까지 여전히 기본 사용자 이름과 암호를 사용하여 시장에 출시되고 있습니다. 이 방법은 허용할 수 없는 관행이며 중단해야 합니다. 고유하고 변경할 수 없는 ID를 사용하여 장치 보안을 한층 더 강화할 수 있습니다.

CVD(Coordinated Vulnerability, 협정 취약성 공개)에 대한 지침2: CVD는 ISO(국제 표준화 기구)에서 표준화했으며 이행이 간편하며 전 세계 일부 대규모 소프트웨어 기업에서 성공적으로 입증되었습니다.[8] 그러나 CVD는 IoT 업계에서는 아직 확립되지 않았으며 일부 회사는 보안 연구원과 상대하는 것을 꺼려할 수도 있습니다. CVD는 보안 연구원이 보안 문제를 알리기 위해 회사에 연락할 수 있는 수단을 제공합니다. 따라서 악의적인 악용 위협을 회사에 사전에 알리고 일반 사용자에게 공개하기 앞서 취약성을 해결할 수 있는 기회를 제공합니다.

인터넷에 연결된 장치와 서비스를 제공하는 기업은 CVD 프로그램을 적용하지 않아 피해를 입을 수 있는 제3자에게 주의를 기울여야 합니다. 또한 산업 기관을 통해 이 정보를 공유하는 회사는 동일한 문제로 어려움을 겪고 있는 다른 사람들을 도울 수 있습니다.

상황에 따라 공개 방법이 달라질 수 있습니다:
단일 제품 또는 서비스와 관련된 취약성: 이 문제는 영향을 받는 이해관계자에게 직접 보고되어야 합니다(예: 장치 제조업체, IoT 서비스 공급자 또는 모바일 애플리케이션 개발자). 이러한 보고서의 출처는 보안 연구원이나 업계 동료일 수 있습니다. 장치 제조업체 또는 기타 영향을 받는 이해관계자와 연락한 후 해당 담당자가 적시에 조치를 취하지 않으면 NCSC에 직접 문제를 보고할 수 있습니다.

시스템 구조적 취약성: 장치 제조업체 등과 같은 이해관계자가 잠재적인 시스템 구조적 문제를 발견할 수 있습니다. 장치 제조업체의 자체 제품에서 문제를 해결하는 것도 중요하지만 이 정보를 공유하면 업계 및 소비자에 상당한 이점이 있습니다. 마찬가지로 보안 연구원도 이러한 시스템 구조적 취약성을 보고할 수 있습니다. 이 경우, 관련 관할 산업

[8] International Organization for Standardization(국제 표준화 기구), 2014, 'ISO/IEC 29147 - Vulnerability Disclosure(ISO/IEC 29147 - 취약성 공개)', https://www.iso.org/standard/45170.html

기관은 보다 광범위한 대응 조치를 취할 수 있습니다. NCSC는 공동 대응 조치를 제공하기 위해 관할 산업 기관에 자문과 안내를 제공할 수 있습니다.

취약성을 해결하기 위한 "시기 적절한 방식"은 매우 다양하고 문제마다 다르지만 취약성 프로세스 완료는 90일을 초과하지 않는 것이 사실 상 표준입니다. 하드웨어 수정은 소프트웨어 수정보다 훨씬 더 오래 걸릴 수 있습니다. 또한, 장치에 배포해야 하는 수정 사항은 서버 소프트웨어 수정과 비교할 때 시간이 더 걸릴 수 있습니다.

소프트웨어 최신 업데이트 유지에 대한 지침3: 소프트웨어 보안 업데이트는 회사의 소비자와 광범위한 기술 에코시스템을 보호할 수 있는 가장 중요한 사항 중 하나입니다. 취약성은 보안과 관련되지 않는 것으로 간주되는 소프트웨어 구성 요소에서 종종 발생합니다. 따라서 일반적인 원칙에 따라 모든 소프트웨어를 최신 상태로 유지되고 적절하게 유지 관리해야 합니다. 수정 사항은 종종 자동 업데이트의 일부로 예방 차원에서 장치에 푸시되며 보안 취약성이 악용되지 않도록 제거할 수 있습니다. 특히 클라우드 업데이트, 장치 업데이트 및 기타 서비스 업데이트가 있을 경우 이 관리 작업은 복잡해질 수 있습니다. 따라서 명확한 관리와 배포 계획이 필수이며 소비자에게 현재 업데이트 상태에 대해 투명하게 제공해야 합니다.

대부분의 경우 소프트웨어 업데이트 게시에는 하위 구성 요소 제조업체와 같은 다른 조직의 여러 종속 관계가 포함됩니다. 이러한 종속 관계는 업데이트를 보류할 이유가 되지 않습니다. 실무 지침은 소프트웨어 공급망 전체에 걸쳐 긍정적인 보안 변화를 장려하는 것이 목적입니다. 장치에 패치를 적용할 수 없는 경우도 있습니다. 일부 매우 제한적인 장치가 이 범주에 해당하며 이러한 범주에 대해서는 대체 계획을 세워 소비자에게 명확하게 전달해야 합니다. 이 계획에서는 기술을 교체해야 할 시기와 해당되는 경우 하드웨어 및 소프트웨어 지원 종료 시기에 대한 일정을 자세하게 제시해야 합니다.

장치가 계속 작동하는 것은 소비자에게 매우 중요할 수 있습니다. 따라서 가능하면 업데이트가 "장치의 기능에 영향을 주지 않아야" 합니다. 특히, 안전 관련 기능을 수행하는 장치의 업데이트는 완전히 해제해서는 안됩니다. 예를 들어 난방 시스템 또는 도난 경보기 작동 유지와 같은 최소한의 시스템 기능이 있어야 합니다. 또한 이러한 유형의 장치 제조업체는 복구 성능이 더 뛰어난 아키텍처로 전환하는 것을 고려해야 합니다.

소프트웨어 업데이트 메커니즘은 공격 벡터이므로 보안이 유지되는지 주의를 기울여 확인해야 합니다.

안전한 통신에 대한 지침5: 보안 제어와 암호 사용의 적합성은 사용 상황을 비롯한 여러 요인에 따라 달라집니다.[9] 보안이 끊임없이 발전하여 암호화 방법에 대한 지침은 빠르게 구식이 되어가는 상황이므로 규범적 지침을 제공하는 것이

[9] 예를 들어 https://www.ncsc.gov.uk/guidance/tls-external-facing-services에서 NCSC의 안내를 볼 수 있습니다.

어렵습니다. 따라서 시행 조직이나 기업은 자사 제품이 암호화 공격에 대한 내성을 유지하면서 사용자 요구를 충족시키도록 보장해야 합니다.

소프트웨어 무결성 보장에 대한 지침7: IoT 장치가 소프트웨어 관련 문제가 발생한 것을 감지한 경우 담당자에게 알릴 수 있어야 합니다. 경우에 따라 장치가 관리 모드에 있을 수 있습니다. 예를 들어 실내의 온도조절장치에 사용자 모드가 있어 다른 설정이 변경되는 것을 방지할 수 있습니다. 이러한 경우 해당 사용자가 알림에 대처할 수 있으므로 관리자에게 알리는 것이 적절합니다.

운영 중단 시 시스템 복원에 대한 지침9: 이 지침의 목적은 개인 안전과 관련된 기능을 비롯하여 소비자 생활의 모든 면에서 IoT 장치 사용이 증가함에 따라 IoT 서비스가 지속적으로 유지되고 실행되도록 하기 위한 것입니다. 예를 들어 커넥티드 도어의 인터넷 연결이 끊어져 밖에서 잠긴 경우 사람들의 생활에 미치는 영향이 상당할 것입니다. 또 다른 예로, 클라우드 서비스에 대한 DDoS 공격 때문에 가정용 난방 시스템이 꺼지는 경우입니다. 다른 보안 관련 규정이 적용될 수 있음에 유의하는 것이 중요하지만 이러한 문제의 원인이 되는 중단을 방지하는 것이 핵심입니다.