SOLAR-OT가 배치한 CHIYU 센서에 발생한 사고 후 교정 조치

최신 버전의 펌웨어 배치 및 SOLAR-OT 감시 플랫폼 강화

작성자	승인자
Deirdre STARSKY, 기술 프로젝트 책임자	Elena PIZARI, 산업 담당 관리 이사

제목

이 문서에는 SOLAR-OT에서 배포한 액세스 제어 시스템에 발생한 사고 후 이행할 다음의 2가지 교정 조치가 자세히 설명되어 있습니다.

1. 모든 시스템에 펌웨어 업데이트 긴급 배포
2. 감시 플랫폼 환경 설정 강화

1. 펌웨어 업데이트 긴급 배포

건설업체 CHIYU에서 취약성을 시정하는 'SEMAC' 액세스 제어 시스템의 펌웨어 업데이트를 개발했습니다 => SOLAR-OT로 모든 사이트에 긴급 배포해야 합니다

SEMAC S2(태양광 발전 단지의 67%)에 배포할 펌웨어 버전 번호는 670VYJLN입니다.

SEMAC S3V3(태양광 발전 단지의 33%)에 배포할 펌웨어 버전 번호는 628AUYSD입니다.

2. 감시 플랫폼 환경 설정 강화

환경 설정

목적은 필수 서비스와 장비만 설치하여 공격을 감행하는 데 사용될 수 있는 기술적 요소를 제한하는 것입니다.

다음과 같은 조치를 통해 보안 수준을 강화합니다.

- 플랫폼 기능 제한
- 플랫폼의 물적 요소 제어

A. 기본 환경 설정 변경

각 구성 요소는 다음을 포함한 표준에 따라 구성됩니다.

- 기술 계정 및 관련 인증 요소
- 사용되는 네트워크 포트
- 설치 및 작업 디렉토리
- 디렉토리 및 파일에 대한 액세스 권한
- 서비스 또는 프로세스를 실행하는 데 사용되는 계정 및 이 계정과 관련된 권한
- 보안 요소, 특히 추적 가능성에 대한 구성 파일

B. 액세스할 수 있는 기능의 제한

플랫폼 운영 및 보안에 필수적인 모듈만 유지 관리하며 적절한 환경 설정, 정기 유지보수 및 감시를 실시해야 합니다.

따라서 운영자는 플랫폼의 기술적 기능을 분석하여 설치는 했지만 사용하지 않는 서비스 또는 기능을 제외시킵니다.

각 하드웨어 또는 소프트웨어 환경 설정은 기준 환경 설정의 형식으로 인벤토리됩니다.

C. 연결된 요소의 인벤토리

운영자는 플랫폼을 구성하는 요소의 완전한 기술 인벤토리를 수행하고 이를 매핑합니다. 인벤토리에는 영구적으로 또는 일시적으로, 물리적으로 또는 원격으로 플랫폼에 연결할 수 있는 장비(워크스테이션, 서버, 주변 장치 등)가 포함됩니다.

제3자가 플랫폼에 연결하는 경우 운영자는 매핑에 이를 기록하고 위험 분석 시 이를 고려합니다.

D. 완전히 제어된 요소 사용

운영자는 다음을 포함한 요소를 직접 관리합니다.

- 업데이트 배포
- 요소 관리
- 원경 환경 설정

파티셔닝

플랫폼은 다음과 같은 목적으로 각 하위 시스템을 자체 작업으로 제한하여 세분화 논리를 따릅니다.

- 공격 표면 제한
- 발생 가능한 공격 억제
- 피해 영향 제한
- 각 하위 시스템의 보안 수준 조정 허용

파티셔닝은 물리적 수단과 논리적 수단에 모두 적용됩니다.

A. 하위 시스템으로 세분화

다음 기준에 따라 하위 시스템으로 세분화합니다.

- 기능
- 데이터 보호 수준
- 노출 수준
- 보안 수준

하위 시스템 간의 모든 연결은 기능적 필요에 따라 타당성이 입증되어야 합니다.

B. 물리적 파티셔닝

가장 중요한 애플리케이션에 전용 서버 한 대를 배치합니다.

C. 논리적 파티셔닝

서버에 저장된 모든 데이터는 사전에 암호화됩니다. 각 하위 시스템은 자체 암호화 메커니즘을 따릅니다.

하위 시스템 간의 모든 통신은 암호화되고 인증된 가상 사설망을 통해 전송됩니다.

원격 액세스

A. 공용 액세스

공용 액세스는 HTTPS 인증 규약을 따르며 플랫폼은 서버 인증서 제시로 인증됩니다.

플랫폼 사용자 대상으로는 2단계 인증을 수행합니다.

B. 노마드 액세스

모바일 워크스테이션은 플랫폼을 향해 인증 및 암호화된 터널을 설정하도록 구성됩니다. 터널은 비활성화할 수 없으며 인터넷 또는 로컬 네트워크에는 액세스할 수 없습니다.
시스템 파티션과 데이터 파티션을 완전히 암호화합니다.

워크스테이션에는 2단계 인증이 설치되어 있습니다.

네트워크 필터링

파티셔닝 외에 추가로 필터링 메커니즘이 적용됩니다.

A. 필터링 지점

하위 시스템 간의 상호 연결이 경계 및 로컬 필터링이 적용되는 주요 필터링 지점입니다.

B. 필터링 규칙

전역 흐름 매트릭스에는 유효한 필터링 규칙이 포함됩니다. 이 매트릭스는 매년 업데이트됩니다.

C. 필터링 수행

반드시 인증 목록 원칙에 기반한 전용 방화벽을 통해 필터링하도록 합니다.