산업제어시스템의 소스코드 보안 취약점 검증 룰 선정을 위한 평가 기준 개발

김은비*, 최이수* ,한동준*
*주식회사 시네틱스
eunbi.kim@synetics.kr, yisoo.choi@synetics.kr, dongjoon.han@synetics.kr

Development of evaluation criteria for selection of source code security vulnerability verification rules for industrial control systems

Eunbi Kim*, Yisoo Choi*, Dongjoon Han*
*Synetics Corp.

요 약

산업제어시스템은 IT 기술의 발전에 따라 다양한 기기 환경과 네트워크를 적용해 진화하고 있다. 이러한 상황에서 사이버 보안의 위협은 가중되고 있으며, 이를 예방하는 방법의 하나로 산업제어시스템에 탑재되는 소프트웨어의 소스코드 개발 과정에서 보안 취약점을 예방하기 위해 소스코드 보안 룰을 적용하여 위반사항을 제거한다. 본 연구에서는 소스코드 보안 룰에서 적용 우선순위를 선정하기 위한 가이드를 개발한다.

1. 서론

IT 기술의 발전에 따라 폐쇄적 환경에서 운영되던 산업제어시스템의 네트워크를 이용한 연결이 확대되고 이를 기반으로 다양한 종류의 기기가 연결되고 있다. 이와 같은 환경에서 산업제어시스템의 사이버 보안이 강조되고 있으며, 미국 국립표준기술연구소(National Institute of Standards and Technology)는 산업제어시스템 보안 가이드(Guide to Industrial Control Systems Security)[1]를 개발 및 보급하고 있다.

소프트웨어의 소스코드 수준에서도 사이버 보안을 위한 방안이 필요하며, 대표적인 방안의 하나는 보안 룰 기반 정적분석을 통한 소스코드 취약점 식별 및 제거이다.

CERT, CWE로 대표되는 소스코드 보안 룰은 소스코드 취약점에 대한 넓은 범위를 포함하고 있다. 이는 많은 룰을 준수할수록 취약점을 제거할 수 있음을 의미하나, 소프트웨어 개발 공수, 일정, 비용의 제약, 산업제어시스템의 특성, 법적 요건에 따라 적절한 룰을 선택하고 적용할 필요가 있다.

본 연구에서는 미국 국립표준기술연구소의 산업제어시스템 보안 가이드와 주식회사 시네틱스의 보안 프로젝트 수행 경험을 기반으로 산업제어시스템의 소프트웨어를 개발하는 조직이 시스템 및 조직의 특성에 따라 적절한 소스코드 보안 룰을 선정할 수 있는 평가 기준을 연구 및 개발하였다.

2. 산업제어시스템의 특성

산업제어시스템은 전기, 석유, 화학, 운송 등의 산업 분야에서 설비나 공정을 감시하고 제어하는 시스템을 의미한다[1]. 감시 제어 및 데이터 수집 시스템, 분산 제어 시스템, 프로그래밍 가능한 로직 제어기 등으로 구성된다. 설비나 공정의 상태를 지속적으로 확인하여 문제 발생을 최소화하려는 목적으로 사용하며, 일반적으로 산업제어시스템의 적용되는 산업 환경에서 설비나 공정에 계획하지 않은 중단이 발생하는 경우 생산 손실 외에 인간 및 환경에 직접적인 영향을 줄 수 있다.

전통적인 산업제어시스템은 물리/논리적으로 격리된 환경에서 동작한다는 특성이 있었으나, IT 기술의 발전 및 비용적인 요인으로 네트워크 연결 및 범용 장비의 사용을 통해 일반적인 IT 시스템과 유사해지고 있으며, 이에 대한 사이버보안 대처가 중요성이 증가하고 있다.

3. 산업제어시스템 보안 가이드

산업제어시스템 보안 가이드는 미국 국립표준기술연구소가 미연방 정보보안 현대화법에 따라 개발한 가이드로, 2015년 2차 개정판이 발행되었다. 산업제어시스템에 대한 소개를 포함하여, 총 6개 항목을 다루고 있으며, 산업제어시스템 위험 관리 및 평가, 보안 구조, 보안 통제 적용에 대한 가이드를 포함하고 있다. 국내에서는 한국인터넷진흥원에서 우리말 번역본[2]을 제공하고 있다.

4. 소스코드 보안 룰셋

소스코드의 보안 취약점 회피를 위한 대표적인 보안 룰셋은 CERT[3]와 CWE[4]가 있다.

CERT는 미국 카네기멜론 대학교에의 소프트웨어 공학연구소(SEI)에서 개발한 소스코드 보안 룰셋이다. 보안 취약점 회피를 목적으로 하며, C언어의 경우 Rule과 Recommendation으로 심각도를 구분한 룰을 총 306개 제공한다.

CWE는 MITRE 개발한 소스코드 보안 룰셋으로, 추상정도에 따라 구분한 룰을 총 81개 제공한다. 공통적인 소프트웨어 취약점들의 리스트 제공을 목적으로 2019년 이후 매년 가장 위험한 소프트웨어 취약점 25개를 CWE Top 25로 발표하고 있다[5].

5. 소스코드 보안 룰 선정 평가 기준 개발

미국 국립표준기술연구소의 산업제어시스템 보안 가이드와 관련 표준/가이드, 주식회사 시네틱스의 사이버 보안 적용 경험에 기반하여 16개 요소가 포함된 룰 선정 평가 기준을 개발하였다.

산업제어시스템은 감시/분산 제어, 데이터 수집, 통신 등의 설계 결정사항을 기반으로 설계된다. 이러한 설계 결정사항들은 시스템 설계에 영향을 끼치므로, 시스템의 보안 여부를 판단하는데 도움을 줄 수 있다[2]. 산업제어시스템 보안 가이드에서는 제어 시간조절 요구사항과 지리적 배급, 계층, 제어 복잡성, 가용성, 결함의 영향, 안전을 산업제어시스템 설계 결정사항을 결정짓는 핵심 요인으로 정의하고 있다.

본 논문에서 제안한 소스코드 보안 룰 선정 평가 기준의 16개 요소는 산업제어시스템 보안 가이드에서 정의한 산업제어시스템 설계 결정사항을 기반으로 시스템 특성, 법 규제, 개발 조직의 역량, 기능 안전 분야 등을 반영하였다. 각 평가기준은 관련도

<표 1> 소스코드 보안 룰 선정 평가 기준

#	요소	정의
1	보안 요구사항 (내부)	보안 요구사항 분석 기법을 통해 도출된 보안 요구사항을 만족해야 하는 정도
2	보안 요구사항 (외부)	발주기관의 보안 요구사항을 만족해야 하는 정도
3	법/제도 규제	국가 기관, 산업계의 보안 법률, 제도 등을 준수해야 하는 정도
4	네트워크 연결	유선/무선 네트워크 연결 여부
5	분산 제어	지역화된 말단 노드(클라이언트)의 중앙 집중식 관리의 필요 여부
6	지리적 배급	지역화된 말단 노드의 지리적 분리 정도
7	적시성	솔루션에서 검출한 문제점의 보고 및 처리의 적시성 정도
8	기능 안전	해당 솔루션의 소프트웨어 기능 오작동으로 인한 인체 피해 여부
9	가용성	솔루션의 다운 타임 허용 정도
10	결함의 영향	솔루션의 오작동 시 발생하는 결함 실패 비용의 정도
11	데이터 저장	솔루션이 검출한 데이터의 저장 필요 여부 및 법적 활용 여부
12	운영 재구축	본 과제 결과물 개발 후, 솔루션 운영을 위한 재개발 불필요 여부
13	구성요소 수명주기	개발한 솔루션이 폐기까지 걸리는 평균 시간(재구축 주기)
14	공급자 연관	솔루션 개발에 포함하는 인증된 3rd Party 솔루션(컴파일러 및 제공 라이브러리, 칩셋 라이브러리 등)을 제외한 소프트웨어 개발 공급자 참여 여부
15	SW 개발 숙련도	소스코드 보안 룰셋 적용을 수행할 SW 개발자와 관리자의 숙련도 정도
16	분석 도구 지원	소스코드 보안 룰셋의 문제점을 분석할 정적분석 도구의 보유 및 지원 정도

에 따라 5점 척도(1점: 매우 낮음 / 5점: 매우 높음)로 평가한다.

총점 80점을 기준으로 평가 결과에 따라 CERT, CWE의 적용 수준을 결정한다. 총점 대비 80% 수준인 64점을 기준으로 Recommendation과 Rule을 모두 적용하며, 64점 미만의 경우 평가기준을 참고하여 적용여부를 결정한다. 단, 시스템의 특성 및 사용하는 정적분석 도구에 따라 룰의 적용을 조정할 수 있다.

<표 2> 평가 결과 점수 구간 별 룰 적용 수준

평가 결과	CERT	CWE
64점 이상	해당 언어 룰 전체 적용	해당 언어 룰 전체 적용
64점 미만	평가기준 참고하여 룰 선정	평가기준 참고하여 룰 선정
20점 이상	Rule 적용	CWE Top 25 적용
20점 미만	적용 필요 여부 검토	적용 필요 여부 검토

6. 소스코드 보안 룰 선정 평가 기준 적용 사례

소스코드 보안 룰 선정 평가 기준을 산업제어시스템인 디지털 사이니지 관련 시스템의 소프트웨어 개발에 적용하였다. 표 4는 소스코드 보안 룰 선정 평가 기준으로 평가한 결과이다.

<표 3> 평가 결과 점수 구간 별 룰 적용 수준

#	룰	검토의견
1	[CERT] ERR34-C Detect errors when converting a string to a number	활용 도구에 따라 적용이 불가능할 수 있음
2	[CERT] FIO 42-C Close files when they are no longer needed	솔루션 특성 상 File Input/ Output에 대한 활용도가 높아 이 룰의 적용은 해당 기능의 적용을 제한할 수 있음
3	[CERT] INT36-C Converting a pointer to integer or integer to pointer	기능 안전과 관련성이 높은 룰로, 솔루션 특성 상 적용이 불필요함
4	[CWE] 401 Missing Release of Memory after Effective Lifetime	의뢰기관에서 적용하는 도구에 적용 불가능함

<표 4> 평가 결과 점수 구간 별 룰 적용 수준

#	평가 기준	평가 점수	평가 근거
1	보안 요구사항 (내부)	5	자체 보안 요구사항 분석을 통해 반드시 만족해야 하는 보안 요구사항 식별
2	보안 요구사항 (외부)	1	발주 기관 등 소요 기관에서의 보안 요구사항 없음
3	법/제도 규제	1	관련 법/제도의 규제가 없음
4	네트워크 연결	5	네트워크 연결이 향후 솔루션 개발의 필수 항목임
5	분산 제어	5	한 대의 서버와 여러 대의 클라이언트(검출 기기)로 구성됨
6	지리적 배급	2	배포 및 문제점 해결은 단일 장소에서 수행 가능함
7	적시성	5	문제 발생 시 즉시 처리 필요
8	기능 안전	1	솔루션 오동작으로 인한 인체 피해 없음
9	가용성	5	디지털 사이니지 동작과 동일한 가용성이 필요
10	결함의 영향	3	결함으로 인한 결함 실패 비용은 평균적임
11	데이터 저장	2	데이터 저장 필요성 또는 데이터 저장의 오류로 인한 문제점 발생 가능성 적음
12	운영 재구축	5	현재 개발 솔루션으로 향후 서비스 예정
13	구성요소 수명주기	5	임베디드 및 산업 기기 특성 상 긴 수명주기를 가짐
14	공급자 연관	1	본 솔루션 개발에 참여하는 외부 소프트웨어 개발 공급자 없음
15	SW 개발 숙련도	4	기능 안전 기기 등 정적 분석 수행 경험 보유
16	분석 도구 지원	3	보안 룰셋 분석 도구를 보유하고 있으나, 제조사의 지원 및 적용 룰셋 지원 부족

평가 점수는 53점으로, 최초 58개의 룰이 적용 대상이었으나, 전문가 검토를 통해 정적분석 도구 지원 여부, 명명 규칙 관련, 솔루션 특성을 고려하여 최종적으로 42개의 룰을 적용하여 소프트웨어를 개

발하였다. 표 3은 전문가 검토를 통해 제외된 룰의 일부를 보여준다.

7. 향후 연구

적용 사례를 통해 다음과 같은 문제점을 식별하였으며, 향후 이에 대한 보완이 필요하다.

- 정량적 평가가 가능하도록 평가 정의 상세화

- 매년 발표되는 CWE Top 25와 개발 언어 별 매핑

또한 본 기준에 따라 보안 룰을 적용한 산업제어시스템의 사이버보안 역량 및 문제점 발생에 대한 지속적인 확인을 통해 본 기준 개발의 타당성을 확인해야 한다.

<사사>

본 연구는 중소벤처기업부와 한국산업기술진흥원의 (지역특화산업육성+(R&D)-지역주력산업육성)으로 수행된 연구 결과입니다.(과제번호 : S2890257)

참고문헌

[1] NIST, “SP800-82 Guide to Industrial Control Systems(ICS) Security,” Rev. 2, 2015

[2] 한국인터넷진흥원, “산업제어시스템(ICS) 보안 가이드”, 2차 개정판, 2020

[3] https://www.sei.cmu.edu/our-work/secure-development/

[4] https://cwe.mitre.org/index.html

[5] https://cwe.mitre.org/top25