Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.2, Apr. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.243

공개 데이터를 활용한 제어시스템 취약점 분석 방안 연구*

신 미 주,[1†] 윤 성 수,[1] 엄 익 채[2‡]
[1,2]전남대학교 (대학원생, 교수)

A Study on the Method of Vulnerability Analysis of Critical Infrastructure Facilities*

Mi-joo Shin,[1†] Seong-su Yoon,[1] Ieck-chae Euom[2‡]
[1,2]Chonnam National University (Graduate student, Professor)

요 약

최근 국가 기반시설에 대한 사이버 공격이 지속해서 발생하고 있다. 이에 따라 ICS-CERT 취약점이 작년보다 두 배 이상이 증가하는 등 원자력 시설 등의 산업제어시스템에 대한 취약점이 날로 증가하고 있다. 대부분의 제어시스템 운영자는 미국의 ICS-CERT에서 제공하는 산업제어시스템 취약점 정보원을 바탕으로 취약점 대응 방안을 수립한다. 그러나 ICS-CERT는 연관된 모든 취약점 정보를 포함하지 않으며, 국내 제조사 제품에 대한 취약점을 제공하지 않아 이를 국내 제어시스템 보안에 적용하기 어렵다. 따라서 본 연구에서는 CVE, CWE, ICS-CERT, CPE 등의 공개된 취약점 관련 정보를 활용하여 제어시스템의 자산에 존재 가능한 취약점을 발견하고 향후 발생 가능한 취약점을 예측할 수 있는 방안을 제안하며, 이를 국내 주요 제어시스템 정보에 적용해보았다.

ABSTRACT

Recently, cyber attacks on national infrastructure facilities have continued to occur. As a result, the vulnerabilities of ICS-CERTs have more than doubled from last year, and the vulnerabilities to industrial control systems such as nuclear facilities are increasing day by day. Most control system operators formulate vulnerability countermeasures based on the vulnerability information sources of industrial control systems provided by ICS-CERT in the United States. However, it is difficult to apply this to the security of domestic control systems because ICS-CERT does not contain all relevant vulnerability information and does not provide vulnerabilities to domestic manufacturer's products. In this research, we will utilize publicly available vulnerability-related information such as CVE, CWE, ICS-CERT, and CPE to discover vulnerabilities that may exist in control system assets and may occur in the future. I proposed a plan that can predict possible vulnerabilities and applied it to information on major domestic control systems.

Keywords: Industrial Control System, Vulnerability, Nuclear facility, ICS-CERT, CVE

Received(02. 08. 2022), Modified(03. 30. 2022), Accepted(03. 30. 2022)

* 본 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(IITP-2019-0-01343)

* 본 논문은 2021년도 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행된 원자력안전연구사업의 연구임(No, 2101061)

* 본 논문은 2021년도 한국정보보호학회 호남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임

† 주저자, shinmj8721@naver.com

‡ 교신저자, iceuom@jnu.ac.kr(Corresponding author)

I. 서 론

산업제어시스템(Industrial Control Systems, ICS)의 디지털화가 진행되며 다수의 제어시스템 운용환경에서 기술지원이나 유지보수를 위해 HMI 등의 장비에 외부로부터의 원격 연결을 허용하고 있고, 이를 악용하여 제어시스템 장비를 조작하는 공격이 증가하고 있다. 이러한 국가 기반 시설에 대한 공격에 효과적으로 대응하기 위해서는 기존에 알려진 제어시스템에 대한 취약점 데이터베이스를 구축하여 선제 대응 체계를 확보해야 한다.

현재 취약점에 대한 데이터를 제공하는 대표적인 기관은 NVD(National Vulnerability Database)[1]와 MITRE[2]가 있으며, 산업제어시스템에 대한 표준화된 취약점 데이터 정보원은 CISA에서 제공하는 ICS-CERT 권고[3]가 대표적이다. 하지만 해당 정보원들은 해외 제조사의 자산과 관련된 취약점 정보는 포함하고 있으나, 국내 제조사의 제어시스템 자산과 관련된 취약점 정보는 포함하고 있지 않다. 국내에서는 한국인터넷진흥원의 'KrCERT'가 국내 소프트웨어 취약점 정보[4]를 제공하지만, 해당 정보는 2018년부터 현재까지 단 113건의 취약점 정보를 제공하며, 이조차도 소프트웨어에 대한 취약점에 제한되어 있다.

국내외 취약점 정보원을 통해서는 국내 제어시스템에 사용되는 국내 제조사의 설비에 대한 취약점 파악이 쉽지 않아, 적합한 대응 체계를 수립하기에는 무리가 있다. 따라서 본 연구는 국내 제어시스템의 자산에 대한 취약점을 분석하고 예측할 수 있는 통합 취약점 분석 방안을 제안하고자 한다.

II. 관련 연구

2.1 취약점 정보원

현재 활용되는 대표적인 취약점 정보원은 NVD에서 제공되는 상용 취약점 정보(Common Vulnerabilities and Exposures, CVE)[5]와 취약 자산 식별 명명 체계(Common Platform Enumeration, CPE)[6]가 있으며, MITRE에서 제공되는 소프트웨어 취약점 정보(Common Weakness Enumeration, CWE)[7]와 공격 패턴 정보(Common Attack Pattern Enumeration and Classification, CAPEC)[8]이 있다. 산업제어시스템에 대한 표준화된 취약점 데이터 정보원으로는 CISA(Cyber security and Infrastructure Security Agency)에서 제공하는 ICS-CERT 권고[3]가 대표적이다.

2.2 취약점 분석 관련 연구

취약점 정보를 통합하여 장비에 대한 취약점을 분석한 다양한 연구들이 수행되었다. 특히 제어시스템에 대한 취약점은 ICS-CERT 취약점 정보원을 사용한 경우가 있었으며, 혹은 사이버 보안 가이드를 바탕으로 취약성을 점검한 연구가 있었다.

제어시스템의 취약점과 관련 데이터를 통합한 연구는 대표적으로 Tomas. RJ 등[9]이 있다. 이는 CISA에서 제공한 ICS-CERT 권고에 근간하여 산업제어시스템에 특화된 취약점 데이터베이스를 구축하였다. 하지만 해당 연구에서 구축한 취약점 데이터는 국내 제품에 대한 취약점을 담고 있지 않아 국내 제어시스템 자산에 대한 취약점을 분석할 수 없다.

또한, 해당 연구에서는 ICS-CERT와 CVE, CWE와의 연관성은 담고 있으나, CPE, CAPEC 등의 관련 정보와의 세부적인 연결성이 미흡하다.

김시원 등[10]은 원자력시설 핵심디지털 자산에 대해 사이버 보안 가이드를 바탕으로 취약성을 점검하였으나, 기존의 상용 취약점 정보나 소프트웨어의 취약점 정보에 관한 정보를 담고 있지 않다. 김민철 등[11]은 CVE, CWE, CAPEC의 공개된 취약점 정보를 통해서 상용 소프트웨어의 취약점 분석 자동화 시스템을 구축하였으나, 해당 시스템은 산업제어시스템과 관련된 취약점 자산을 사용하지 않아 산업제어시스템의 취약성을 평가하기에는 어려움이 있다. 김희현 등[12]은 국내 산업제어시스템에 적용 가능한 취약점 분류 체계를 제안하였으나 이는 웹 취약점에 제한되어 포괄적으로 제어시스템의 취약점 분석에 적용하기에는 어려움이 있다.

Table 1. Data features of Vulnerability Information Sources in Related Studies

paper	Data features				
	ICS	CVE	CWE	CPE	CAPEC
[9]	●	●	●		
[10]	●				
[11]		●	●		●
[12]	●		●		

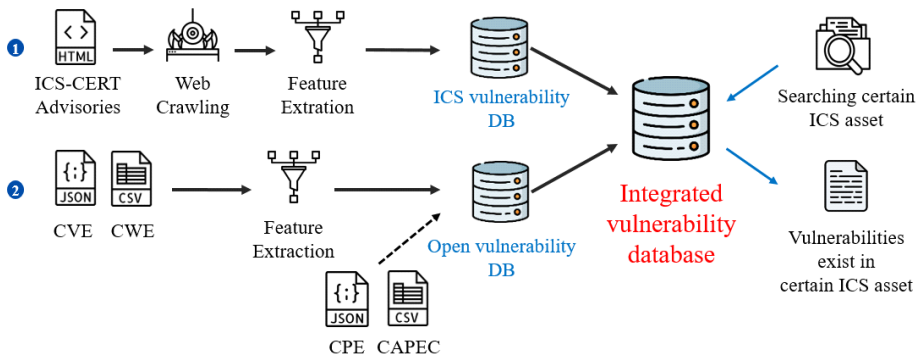

Fig. 1. Vulnerability analysis workflow

III. 제안하는 취약점 분석 및 예측 방안

본 논문에서는 Tomas. RJ 등[9]을 참고하여 ICS-CERT 권고, CVE, CWE 공개된 취약점 데이터를 반영하여 연관된 취약점 정보를 파악할 수 있도록 한다. 또한 기존 연구에 CPE와 CAPEC의 데이터를 추가하여 CPE 기반의 자산 식별 방법론과 자산에 대한 취약점 분석 방법론을 새롭게 제안한다. 또한 CWE를 사용하여 발견되지 않은 취약점에 대하여 예측 할 수 있는 방법론을 제안한다.

이를 위해 3.1에서는 제어시스템 설비의 취약점 분석과 예측을 위한 데이터베이스를 구축하는 방법을 서술한다.

3.2에서는 국내 제어시스템의 자산을 식별하기 위한 CPE 기반의 자산 식별 방법론을 제안한다.

3.3에서는 3.2의 방법론을 사용하여 식별한 제어시스템 자산에 대하여 3.1에서 구축한 취약점 데이터베이스를 이용하여 자산에 대한 취약점을 분석하는 과정을 설명한다.

3.4에서는 더 나아가 식별된 제어시스템 자산의 발생 가능한 취약점을 예측하는 방법론을 설명한다.

3.1 취약점 데이터베이스 구축

본 연구는 CISA에서 제공하는 현재 산업제어시스템의 보안 문제, 취약성 및 악용에 대한 적시 정보인 ICS-CERT 권고(Advisories)를 이용하여 산업제어시스템에 대한 전반적인 취약점 정보를 수집한다.

Fig. 1.과 같이 CISA의 웹 페이지에서 ICS-CERT 권고 정보를 크롤링하여 취약점이 발생한 장비의 이름, 제조사, 영향 받은 제품의 목록과 해당 취약점에 대한 CVE, CWE 등의 정보 등 필요한 정보를 추출하고 이를 산업제어시스템 취약점 정보 데이터베이스에 저장한다. 이는 첫 번째 동기화 시점으로써 1~7일 간격으로 업데이트되는 권고 정보를 수동 및 자동으로 동기화 하여 주기적으로 새로운 취약점 정보를 갱신 할 수 있도록 한다. 또한, 국내 원자력 제어시스템의 특징을 반영하기 위해 국내 원자력 제어시스템의 자산 유형 정보를 추가하여 권고에서 제공하는 취약점의 자산 유형이 국내의 자산 유형에 대응될 수 있도록 한다. 권고에서 세부적으로 다루지 않는 상용 취약점 정보인 CVE와 소프트웨어 취약점 정보인 CWE는 두 번째 동기화 시점을 통하여 공개 취약점 정보 데이터베이스를 구축한다.

산업제어시스템 취약점 정보와 공개 취약점 정보를 통합하여 통합 산업제어시스템 취약점 데이터베이스를 구축하여 사용자가 자산 유형을 조회했을 때 산

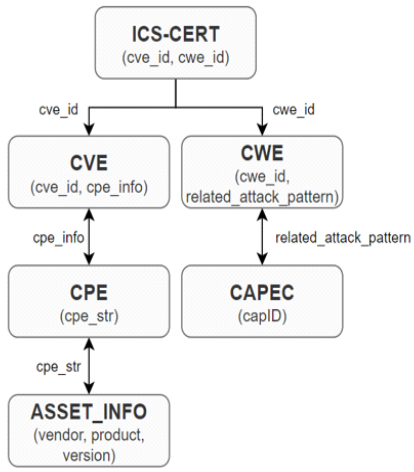

Fig. 2. Relationships between Database tables

재해 있는 ICS-CERT 권고, CVE, CWE, CPE, CAPEC 에 근거한 취약점 정보를 통합적으로 조회할 수 있도록 한다.

Fig. 2.는 구축한 데이터베이스 테이블 간의 연관성과 속성 정보를 그림으로 나타낸 것이다. 해당 그림을 통해 각 취약점 정보 간의 관계와 외래키, 그리고 CPE와 자산 정보 테이블 간의 관계성을 파악할 수 있다. 이를 통해 하나의 테이블에 속한 정보로 여러 연관된 테이블의 취약점 정보를 제공할 수 있다.

3.2 제어시스템 자산 식별

국내 원자력 제어시스템을 구성하는 자산은 해외 제조사의 제품과 국내 제조사의 제품을 모두 포함하고 있다. 원자력 시설에 대한 취약성을 점검하기 위해서는 원자력 시설을 구성하는 자산에 대한 취약점 검색을 수행해야 하며, 취약점 검색에 사용되는 자산에 대한 정확한 식별이 필수적이다. 따라서 본 연구에서는 취약점을 검색하기 위한 CPE 기반 자산 식별 방법론을 제시한다.

CPE는 NVD에서 발행하는 취약 자산 식별 명명체계로, 현재 약 80만 건의 데이터가 집계되어있다. CPE는 취약한 자산에 대한 식별 정보를 URI 형식으로 제공하며, 그 형식은 Fig. 3와 같다.

URI는 자산의 제조사, 제품명, 제품 버전 등의 정보들을 담고 있다. 이러한 CPE URI는 CVE 취약점의 한 속성으로써 명시되어 자산에 대응하는 CVE 취약점을 찾을 수 있다. Fig. 4.과 같이 상용 취약점 정보인 CVE는 해당 취약점에 영향을 받는 자산을 'cpe_info'에 명세하고 있다.

본 연구에서는 이러한 CPE와 CVE의 관계성을 이용하여 자산을 정확하게 식별하고 취약점을 탐색한다.

사용자는 원자력 시설에 대한 자산 정보를 입력할 때 제안하는 CPE 기반의 입력 체계를 사용한다. 사용자가 〈제조사〉를 입력하면 입력한 제조사 정보를 CPE 테이블에 검색하여 대응하는 제품 리스트를 찾는다. 탐색한 제품 리스트를 드롭다운 형식으로 사용자에게 제공하여 사용자가 제품명을 고를 수 있도록 한다.

cpe:2.3:part:vendor:product:version:update:edition:language:sw_edition:target_sw:target_hw:other

Fig. 3. CPE URI format

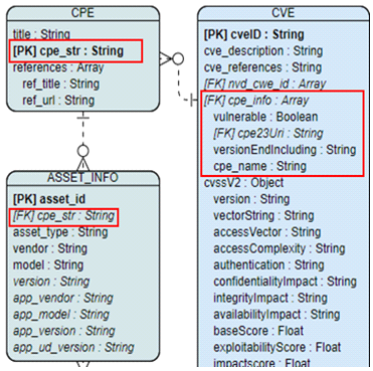

Fig. 4. Relevance between CPE and CVE

사용자가 입력한 〈제조사, 제품명〉을 다시 CPE에 테이블에 검색하여 대응하는 버전 정보를 찾는다. 탐색한 정보에서 사용자가 버전 정보를 선택하여 자산 정보를 입력할 수 있도록 한다. 입력된 CPE 기반의 자산 정보는 데이터베이스에 저장하여 해당 자산에 대한 취약점을 탐색할 때 사용한다.

3.3 취약점 분석

Fig. 5.는 본 논문에서 수행하는 취약점 분석 절차이다. 이를 통해 제어시스템 자산의 제조사에 구애받지 않고 통합적으로 취약점을 분석할 수 있다.

CPE 기반으로 입력된 자산 정보를 CVE 테이블의 'cpe_info'에 검색하여 대응하는 CVE 취약점을 찾을 수 있다. 또한 ICS-CERT 테이블에 해당 정보를 검색하여 대응하는 ICS-CERT 취약점을 찾을 수 있다.

하지만, CVE와 ICS-CERT에도 대응되지 않는 자산 정보가 존재할 수 있다. 대부분의 국내 제조사의 자산 제품군이 여기에 해당하는데, 이 경우에는 자산에 탑재된 어플리케이션 정보를 추가로 입력한다. 자산에 탑재된 소프트웨어, 운영체제 정보를 입력하고, 해당하는 제품에 대한 CVE를 검색한다면 자산에 탑재된 어플리케이션의 취약점을 탐색할 수 있다.

Table 2.를 통해서 2가지 활용 사례를 확인할 수 있다. 첫 번째 자산인 GE의 PLC 제품은 자산에 탑재된 상용 시스템 정보를 입력하지 않았다. 하지만 해당 제어시스템 자산의 제조사와 제품명 2가지 속성으로 ICS-CERT 기반의 검색 수행 시 해당 자산에 대한 취약점을 찾을 수 있다. 또한 ICS-CERT

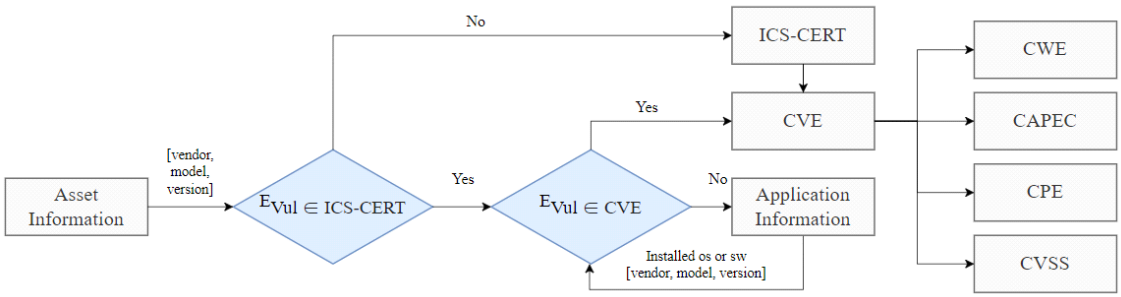

Fig. 5. Proposing vulnerability analysis process

Table 2. Vulnerability sources based on asset information. T is a type, V is a vendor of asset, M is a model name of asset, R is a version of model, U is an update information of asset. Vul Sources means which database the vulnerability exists in.

Asset Type	Asset information (ICS-CERT based vulnerability search)			Application information of asset (CPE-CVE based vulnerability search)				Vul Sources
	V	M	R	V	M	R	U	
PLC	GE	Mark vie	*	*	*	*	*	- ICS-CERT - CVE, CWE
PLC	Soosan	POSAFE-Q	*	black berry	qnx_software_development_platform	6.4.1	*	- CVE, CWE

와 연관된 CVE, CWE를 통해서 통합 취약점 정보를 제공할 수 있다.

두 번째 자산은 국내 제조사의 제품으로, ICS-CERT 기반 탐색이 불가능하다. 이런 경우에는 해당 제품에 탑재된 상용 시스템 정보를 바탕으로 취약점을 탐색한다. 운영체제 제조사, 제품명, 버전에 대한 속성이 CPE 형식으로 입력되어 있기 때문에 이와 대응되는 CPE URI를 찾아낼 수 있다. 그리고 특정된 CPE URI를 CVE 정보원의 'cpe_info' 속성값 집합과 대조하여 해당하는 CVE와 연관된 CWE를 탐색할 수 있다.

3.4 취약점 예측

제어시스템을 구성하는 자산에 대한 취약점 발생을 예측하는 방법은 크게 인공지능을 사용하는 제로데이 취약점 예측과 분석적 통계적 방법을 이용한 추론적 예측이 있다.

[13]은 NVD 데이터를 바탕으로 다음 취약점 발생까지의 시간을 예측하여 위험 평가를 수행하였다. CVE에서 가장 많은 취약점을 가지고 있는 상위 6개의 제조업체를 선별하여 각 제조사별 인공지능 모델을 구축하였다. Linux, Sun, Cisco, Mozilla, Microsoft, Apple의 제품군에 대하여 CVE가 발행된 날짜 간의 간격을 피처로 사용하여 다음 취약점이 발생할 시간을 예측했다. 이는 상용시스템 취약 자산에 대한 취약점 예측 방안이며, 본 연구에서 적용 시 제어시스템의 자산에 대한 취약점 정보가 충분치 않기에 인공지능 학습을 통한 예측의 정확도 면에서 한계를 가진다.

[14]는 NVD의 취약점 데이터와 CWE 사이의 관계를 분석함에 따라 추론적 방법론을 사용하였다. 이때 한 취약점이 다른 취약점의 결과로써 작용하는 점을 이용하여 '제로데이' 시간을 계산하였다. 이때 Siemens 제품에 대한 CVE 207개에 대한 CWE를 분석하여 해당 취약점이 제로데이 취약점으로써 남아있던 기간을 추론하였다. 결과적으로 Siemens 제품 릴리즈와 CVE 공개 사이의 최소 기간은 115일, 최대 기간은 14.7년임을 파악했다.

본 연구에서는 [14]를 바탕으로 CWE를 이용하되, 결함 집중원리를 기반으로 이전 취약점의 상위 10개의 CWE로 다음 취약점을 예측하는 방안을 제안한다.

CWE는 아키텍처, 설계, 구현 단계에서 발생할 수

있는 소프트웨어 및 하드웨어의 보안 취약성에 대해 공통적으로 적용할 수 있도록 체계적으로 분류한 카탈로그이다.[15] 특정 제조사의 제품군은 결함 집중 원리에 따라 대다수의 결함들이 소수의 특정 모듈에 집중하여 발생하는 경향이 있다. 해당 결함은 취약점으로 발현되기도 하며, 발현된 취약점들은 근본 원인인 CWE로 분류된다. 그리고 세부적인 취약점은 CVE로 명명된다. CWE는 공급업체로부터 더 많은 정보를 받아 생성되기 때문에 일반적으로 실제 취약성에 더 정확하다.[14] 이를 바탕으로 어떠한 자산에서 발생할 취약점은 그 제조사 제품군에서 자주 발생하는 CWE에 기반 함을 알 수 있다.

3.1에서 구축한 취약점 데이터베이스에서 산업제어시스템 자산 관련 취약점인 ICS-CERT 취약점 1800개를 분석하였다. Fig. 6.과 같이 Siemens 社의 제품에 대한 취약점이 300건 이상으로 전체의 5%를 차지하며 가장 많은 취약점을 가진 것으로 집계되었다. 이때 Siemens 장비의 CWE 집계 현황을 보면, Fig. 7.과 같이 가장 많이 집계된 상위 10개의 CWE가 전체의 약 80%를 차지하는 것을 알 수 있다. 이를 바탕으로 해당 제조사에서 출현한 CWE 중 가장 많이 집계된 CWE를 예방할 수 있다면 해당 제조사 제품군의 취약점을 예측할 수 있다.

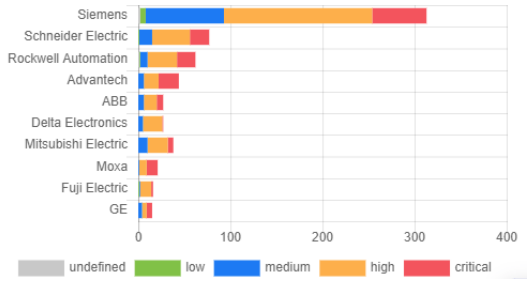

Fig. 6. Number of ICS-CERT vulnerabilities by vendor

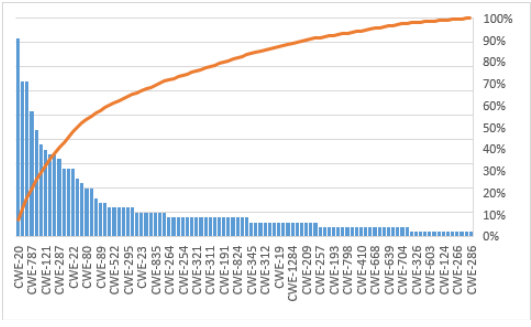

Fig. 7. CWE distribution graph for Siemens products

상위 10가지의 CWE를 찾는다면 Fig. 2.에서 나타난 CWE와 CVE의 관계에 따라 상위 10개의 CWE에 대응하는 CVE를 찾을 수 있다. 해당 취약점은 제조사의 제품군에서 발생 가능한 취약점으로 분류하여 제어시스템의 자산을 관리할 수 있다.

IV. 취약점 분석 및 예측 실험

4.1 취약점 분석

본 연구에서 제시하는 취약점 분석 방법론에 대한 효과성을 검증하기 위하여 실제 자산 23개에 대한 취약점 분석을 실시하였다. 분석 과정에 사용되는 자산은 국내 기반 시설에 쓰이는 자산으로 이루어져있다.

기존 연구들이 수행한 취약점 분석 방법을 사용했을 경우, Table 3.과 같이 총 14개의 자산에 대한 취약점을 찾을 수 있었다. 하지만 9개의 자산에 대한 취약점은 ICS-CERT와 CVE 에서는 찾을 수 없다.

이때 본 논문에서 제시하는 취약점 분석 방법론과 같이 자산에 탑재된 상용 시스템에 대한 명세를 자산 명세와 함께 검색한다면 Table 4.와 같이 9개의 자산 중 탑재된 어플리케이션 정보를 식별할 수 없는 3개의 자산을 제외한 6개의 자산에 대한 취약점을 추가로 찾을 수 있다. 이때 특히 국내 제어시스템에 주로 사용되는 국내 PLC 제조사 A 社의 PLC 장비에 대한 취약점을 탑재된 상용 시스템에 대한 정보로 찾을 수 있다.

4.2 취약점 예측

본 연구에서 제안하는 취약점 예측 방법론을 실험하기 위하여 4.1의 취약점 평가 대상 목록 중 Siemens, Adventech, Schneider 社에 대한 잠재적 취약점을 분석하였다. Fig. 8은 2018년부터 2020년 까지 발생한 Top 10 CWE 데이터를 A로, 2021년부터 2022년 까지 발생한 Top 10 CWE 데이터를 B로 나누어 각 CWE의 분포도를 나타낸 것이다.

Siemens 社의 제품에서 발생한 취약점의 경우, A에서 발생한 대부분의 CWE가 B에서도 발생했다. A와 B 모두에 속하는 CWE는 400, 125, 787,

Table 3. Vulnerability searching result for real assets in ICS (Because of the security of The Critical Infrastructure, Product name of the real assets were masked.)

Index	Vendor	Product	ICS-CERT matching	CPE-CVE matching
1	ABB	ACXXX	-	-
2	Advantech	WebAccess/SCADA	11	32
3	Advantech	iView	4	11
4	BlackBerry	QNX OS	1	1
5	CentOS	Centreon	-	17
6	Cisco	Firepower XXXX Series	-	14
7	Emerson/WEC	Ovation Controller OCR XXX	-	-
8	GE	Speedtronic Mark XX	2	-
9	Lenel S2	OnGuard Access Control	-	-
10	Mitsubishi	Air controller	2	2
11	MOXA	Nport XX	2	11
12	Omoln	CVXXX CPU	-	-
13	OPC Foundation	OPC UA	1	3
14	OWL cyber defense	OPDS-XXX	-	-
15	Rosemount	3XXX Pressure Transmitter	-	-
16	Schneider	EcoStruxure Control Expert	2	5
17	Siemens	SIPROTEC XX relays	2	3
18	Siemens	SCALANCE XXX	4	3
19	Siemens	SIMATIC S7XXX	2	-
20	Domestic PLC vendor A	POSAFE-Q	-	-
21	Waterfall	WF-XXX Security Gateways	-	-
22	Domestic PLC vendor B	OPERASYSTEM XXX	-	-
23	Suprema	Biostar X	-	1

Table 4. Vulnerability researching result by application information for fault assets in Table 3 (Because of the security of The Critical Infrastructure, Product name of the real assets were masked.)

Index	Vendor	Product	Application info	CPE-CVE matching
1	ABB	ACXXX	VRTX(RTOS)	5
7	Emerson/WEC	Ovation Controller OCR XXX	Windows CE(RTOS)	9
9	Lenel S2	OnGuard Access Control	Windows 2000	50
12	Omoln	CVXXX CPU	RX116	11
14	OWL cyber defense	OPDS-XXX	redhat	62
15	Rosemount	3XXX Pressure Transmitter	-	-
20	Domestic PLC vendor A	POSAFE-Q	qnx software	10
21	Waterfall	WF-XXX Security Gateways	-	-
22	Domestic PLC vendor B	OPERASYSTEM XXX	-	-

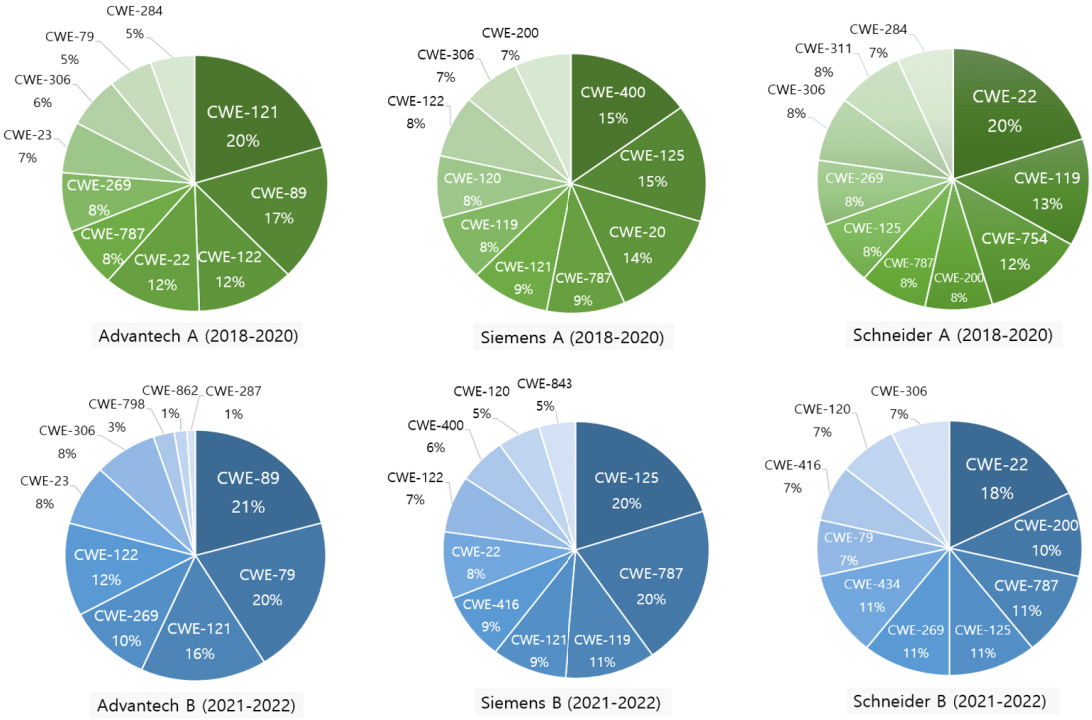

Fig. 8. CWE distribution Pie graph for Advantech, Siemens, Schneider products

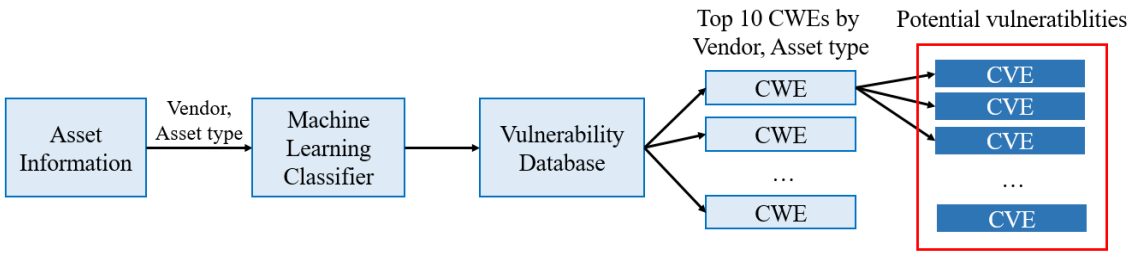

Fig. 9. Proposing vulnerability analysis process

121, 119, 120, 122 으로 B 취약점의 전체의 78%를 차지했다. Advantech 社의 경우에도 A와 B 모두에 속하는 CWE가 121, 89, 122, 269, 23, 306, 79로 B 취약점의 95%를 차지했다. 또한 Schneider 社에서 발생한 취약점을 분석했을 때, A와 B 모두에 속하는 CWE는 22, 200, 787, 125, 269, 306으로 B 취약점의 68%를 차지했다.

이로써 제조사의 제품군에 발생한 취약점 근본 원인을 분석하여 앞으로 발생할 잠재적인 취약점을 예방할 수 있다는 것을 알 수 있다.

4.3 토의

4.1에서는 총 23개의 국내 기반 시설의 취약점 평가 대상 자산에 대하여 기존의 ICS-CERT 기반으로 11개의 자산의 취약점 분석을 수행할 수 있었지만, 제안하는 CPE 기반의 CVE 취약점 검색 방법론으로 추가로 3개 자산에 대한 취약점을 분석했다. 또한, 취약점을 찾지 못한 나머지 9개의 자산에 대하여 본 논문에서 제안하는 탑재된 어플리케이션 정보를 이용한 취약점 분석 방법론을 적용하여 추가로 6개의 자산에 대한 취약점을 찾을 수 있었다.

결과적으로 기존의 취약점 분석 방법론은 48%의

자산에 대해 취약점을 분석하였지만, 제안하는 방법론은 87%의 자산에 대해 취약점을 분석할 수 있었다.

4.2에서는 Siemens, Advantech, Schneider의 세 제조사에 대하여 3.4에서 제시한 취약점 예측 방법론을 적용하였다. 그 결과 각 제조사의 제품군의 이전의 취약점 근본 원인을 바탕으로 발생할 수 있는 취약점을 알아낼 수 있었다.

본 연구에서 제안하는 취약점 예측 방법론을 도식화 하여 Fig. 9.에 나타내었다. 4.2의 실험에서는 자산의 제조사를 기반으로 Top 10 CWE를 도출하였다. 하지만, 이때 취약점을 예측하고자 하는 자산의 제품 유형을 추가한다면 취약점 예측 정확도를 높일 수 있을 것이다. 그 방안은 아래와 같다.

제어시스템에 대한 취약점 데이터베이스인 ICS-CERT 데이터에 대한 자산 유형 라벨링 작업을 수행한다. 자산 유형이 라벨링된 취약점 데이터를 인공지능 분류기에 입력하여 모델을 학습한다. 이때 로지스틱 회귀, 나이브 베이즈, 결정 트리, 서포트 벡터 머신 등의 분류 알고리즘이 사용될 수 있다. 학습된 모델을 이용하여 자산 정보인 〈제조사, 제품명〉을 입력하면 인공지능 분류기를 사용하여 자산 유형을 분류한다. 분류된 자산 유형을 사용하여 현재 ICS-CERT 취약점 데이터에 대응하는 CWE와 취약점을 찾을 수 있을 것이다.

V. 결 론

본 연구가 제안하는 제어시스템 취약점 분석 방안은 ICS-CERT를 기반으로 산재하여 있는 공개 데이터 CVE, CWE 등의 취약점 관련 정보를 통합하였다.

또한 제어시스템에 적용할 수 있는 CPE 기반 자산 입력 체계와 CVE, ICS-CERT를 통한 취약점 분석 방법론을 제안하였다. 이를 이용하여 국내 제조사의 자산에 대한 정보가 ICS-CERT와 CVE에 존재하지 않을 때, 자산에 탑재된 어플리케이션 정보를 이용하여 취약점을 찾을 수 있다.

제어시스템의 자산에 대한 잠재적인 취약점을 예측하기 위해서는 분석적 방법론을 적용하여 CWE를 기반으로 잠재적인 취약점을 예측하는 방법론을 제안하였다.

제안하는 통합 취약점 분석 방안을 이용하여 임의의 실제 취약점 평가 대상 자산 23개에 대한 취약점을 분석한 결과 기존의 ICS-CERT를 통한 취약점 분석은 총자산의 48%에 대하여 취약점을 찾았지만, 제안하는 방법론은 87% 이상의 자산에 대한 취약점을 탐색하였다. 또한 제안하는 취약점 예측 방안을 이용하여 Siemens, Advantech, Schneider의 2018년에서 2020년의 취약점 근본 원인을 바탕으로 2021년부터 2022년까지의 취약점 예측을 수행하였다.

본 연구가 제안하는 취약점 분석 및 예측 방안을 실제 제어시스템에 적용하면 높은 정확도로 필수 디지털 자산에 대한 취약점을 분석할 수 있으며, 잠재적인 취약점을 예측할 수 있을 것이다.

References

[1] NVD Vulnerabilities, "National Vulnerability Database" https://nvd.nist.gov/vuln, Apr. 2022.

[2] MITRE CVE, "CVE Data Feeds" https://cve.mitre.org/cve/data_feeds.html, Apr. 2022.

[3] CISA ICS-CERT Advisories, "ICS-CERT Advisories" https://us-cert.cisa.gov/ics/advisories, Apr. 2022.

[4] KrCERT Vulnerability Informations, "KISA Vulnerability Informations" https://www.krcert.or.kr/data/secInfoList.do, Apr. 2022

[5] NVD Data Feed for Vulnerabilities, "NVD CVE Data" https://nvd.nist.gov/vuln/data-feeds Apr. 2022

[6] NVD Official Common Platform Enumeration (CPE) Dictionary, "NVD CPE Data" https://nvd.nist.gov/products/cpe, Apr. 2022

[7] MITRE Common Weakness Enumeration, "Mitre CWE Data" https://cwe.mitre.org/data/downloads.html, Apr. 2022

[8] MITRE Common Attack Pattern Enumeration and Classification, "Mitre CAPEC data" https://capec.mitre.org/data/index.html, Apr. 2022

[9] J.T. Richard and T. Chothia, "Learning from Vulnerabilities - Categorising,

Understanding and Detecting Weaknesses in Industrial Control Systems," International Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems, pp. 100-116, Dec. 2020

[10] In-kyung Kim and Kook-heui Kwon, A Study on Vulnerability Assessment for the Digital Assets in NPP Based on Analytical Methods," Journal of the Korea Institute of Information Security & Cryptology, 28(6), pp. 1539-1552, Dec. 2018

[11] Min-Cheol Kim and Se-Joon Oh, "Risk Scoring System for Software Vulnerability Using Public Vulnerability Information," Journal of the Korea Institute of Information Security & Cryptology 28(6), pp. 1449-1461, Oct. 2018

[12] Hee-Hyun Kim and Jin-Ho Yoo, "A Study on ICS/SCADA System Web Vulnerability," The Jounal of Society for e-Business Studies 24(2), pp. 15-27, Nov. 2019

[13] Xinming Ou and Doina Caragea "Predicting Cyber Risks through National Vulnerability Database," Information Security Journal: A Global Perspective, vol. 24, no.4, pp. 194-206, Nov. 2015

[14] Richard J. Thomas and Joseph Gardiner "Catch Me If You Can: An In-Depth Study of CVE Discovery Time and Inconsistencies for Managing Risks in Critical Infrastructures," CPSIOTSEC'20: Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy, pp. 49-60, Nov. 2020

[15] Sung-Min Kim and Dong-Kwan Kim, "Automatic Detection of Software Security Vulnerabilities," Jonal of The Transactions of the Korean Institute of Electrical Engineers, 70(3), pp. 157-162, Sep. 2021

〈저자소개〉

신 미 주 (Mi-joo Shin) 학생회원
2020년 8월: 전남대학교 소프트웨어공학과 졸업
2020년 9월~현재: 전남대학교 정보보안협동과정 석사
〈관심분야〉 산업제어시스템보안, 취약점연구

윤 성 수 (Seong-su Yoon) 학생회원
2021년 2월: 전남대학교 소프트웨어공학과 졸업
2021년 3월~현재: 전남대학교 정보보안협동과정 석사
〈관심분야〉 정보보호, 인공지능

엄 익 채 (Ieck-chae Euom) 종신회원
2003년 8월: 전남대학교 컴퓨터정보학부 학사
2015년 2월: 한국과학기술원 소프트웨어대학원 석사
2019년 2월: 전남대학교 정보보안협동과정 박사
2019년 10월~현재: 전남대학교 시스템보안연구센터 소장, 조교수
〈관심분야〉 산업제어시스템보안, 데이터 보안, 취약점연구, IoT보안