https://doi.org/10.33778/kcsa.2022.22.1.011

국내 원자력 시설 통합 취약점 분석 프레임워크 연구★

신 미 주*, 윤 성 수**, 엄 익 채***

요 약

최근 사이버 공격으로 인해 발생한 우크라이나 대규모 정전 사태를 비롯하여 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 ICS-CERT에서 제공하는 제어시스템 취약점 정보(1,843건)를 기준으로 해당 취약점과 관련된 CVE, CWE, CAPEC, CPE 정보를 통합한 취약점 분석 프레임워크를 제시한다. 또한 원자력 시설의 자산을 CPE를 이용하여 식별하고 CVE와 ICS-CERT를 이용하여 취약점을 분석한다. 기존의 방법론으로 취약점 분석 시 임의의 국내 원자력 시설 자산 중 ICS-CERT에는 단 8%의 자산에 대한 취약점 정보를 탐색하였지만, 제안하는 방법론을 이용하면 70% 이상의 자산에 대해 취약점 정보를 탐색할 수 있다.

A Study on the Framework of Integrated Vulnerability Analysis of Domestic Nuclear Facilities

Mi-Joo Shin*, Seong-su Yoon**, Ieck-chae Euom***

ABSTRACT

Cyber attacks on national infrastructure, including large-scale power outages in Ukraine, have continued in recent years. As a result, ICS-CERT vulnerabilities have doubled compared to last year, and vulnerabilities to industrial control systems are increasing day by day. Most control system operators develop vulnerability countermeasures based on the vulnerability information sources provided by ICS-CERT in the United States. However, it is not applicable to the security of domestic control systems because it does not provide weaknesses in Korean manufacturers' products. Therefore, this study presents a vulnerability analysis framework that integrates CVE, CWE, CAPE, and CPE information related to the vulnerability based on ICS-CERT information (1843 cases). It also identifies assets of nuclear facilities by using CPE information and analyzes vulnerabilities using CVE and ICS-CERT. In the past, only 8% of ICS-CERT's vulnerability information was searched for information on any domestic nuclear facility during vulnerability analysis, but more than 70% of the vulnerability information could be searched using the proposed methodology.

Key words : Industrial Control System, Nuclear Facility, Integrated Vulnerability Analysis, CVE, CPE

접수일(2021년 11월 30일), 게재확정일(2021년 12월 31일)

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

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

* 전남대학교 시스템보안연구센터 대학원생(주저자)

** 전남대학교 시스템보안연구센터 대학원생(공동저자)

*** 전남대학교 시스템보안연구센터 교수(교신저자)

1. 서 론

산업제어시스템(industrial control systems, ICS)의 디지털화가 진행되며 다수의 원자력 시설 등의 제어 시스템 운용환경에서 기술지원이나 유지보수를 위해 HMI 등의 장비에 외부로부터의 원격 연결을 허용하고 있고, 이를 이용하여 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 정보원으로는 CISA(Cyber security and Infrastructure Security Agency)에서 제공하는 ICS-CERT 권고 [3] 가 대표적이다. 하지만 해당 정보원들은 국외의 기반 시설 자산과 관련된 취약점 정보는 포함하고 있으나, 국내 제조사의 원자력 시설 자산과 관련된 취약점 정보는 포함하고 있지 않다.

국내에서는 한국인터넷진흥원의 'KrCERT'가 국내 소프트웨어 취약점 정보 [4] 를 제공하지만, 해당 정보는 2018년부터 현재까지 단 83건의 취약점 정보를 제공하며, 이조차도 소프트웨어에 대한 취약점에 제한되어 있다.

국외, 국내의 취약점 정보원을 통해서는 국내 원자력 제어시스템에 사용되는 국내 제조사의 설비에 대한 취약점 파악이 어려우므로 국내 원자력 제어시스템에 적용하여 대응 체계를 수립하기에는 무리가 있다.

따라서 본 연구는 국내 원자력 제어시스템의 특징을 반영하여 국내외 제어시스템의 취약점을 포괄할 수 있는 통합 취약점 분석 프레임워크를 제안하고자 한다.

2. 관련 연구

현재 활용되는 대표적인 취약점 정보원은 NVD에서 제공되는 상용 취약점 정보인 CVE(Common Vulnerabilities and Exposures) [5] 와 취약 자산 식별 명명 체계인 CPE(Common Platform Enumeration) [6] 가 있으며, MITRE에서 제공되는 소프트웨어 취약점 정보인 CWE(Common Weakness Enumeration) [7] 와 공격 패턴 정보인 CAPEC(Common Attack Pattern Enumeration and Classification) [8]이 있다.

국내외 관련 선행연구를 분석하여 산업제어시스템과의 관련성과 네 가지 취약점 정보원에 반영 여부를 평가하였다. <표 1>은 산업제어시스템에서의 취약점 분석 연구 혹은 취약점 분석 프레임워크에 대한 관련 연구를 나타낸 것이다.

<표 1> 관련연구의 취약점 정보 특징

연구	취약점 정보 특징				
	ICS	CVE	CWE	CPE	CAPEC
[9]	●	●	●		
[10]	●				
[11]		●	●		●
[12]	●		●		

Tomas, R.J 등 [9] 는 CISA에서 제공한 ICS-CERT 권고에 근간하여 산업제어시스템에 특화된 취약점 데이터베이스를 구축하였다. 해당 ICS-CERT와 CVE, CWE와의 대응 관계는 존재하나 CPE, CAPEC 등의 관련 정보와의 세부적인 연결성이 미흡하다.

김시원 등 [10] 은 원자력 시설 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] 는 국내 산업제어시스템에 적용 가능한 취약점 분류 체계를 제안하였으나 이는 웹 취약점에 제한되어 포괄적으로 제어시스템의 취약점 분석에 적용하기에는 어려움이 있다.

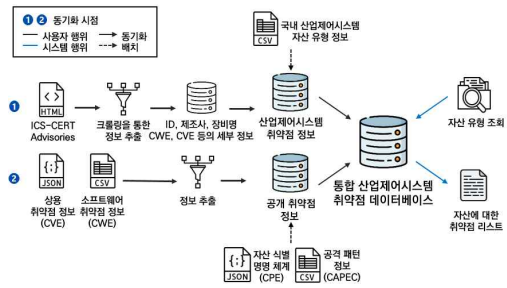
따라서 본 논문에서는 ICS-CERT 권고, CVE, CWE, CPE, CAPEC의 공개된 취약점 데이터를 모두 반영하여 연관된 취약점 정보를 파악할 수 있도록 한다. 또한 국내 제어시스템 자산에 대한 특징을 반영할

수 있도록 새로운 자산 식별 방법론과 자산에 대한 취약점 분석 방법론을 제안하며, 마지막으로 해당 프레임워크의 활용 방안을 소개한다.

3. 통합 취약점 분석 프레임워크

3.1 프레임워크 설계

본 연구에서 제안하는 프레임워크의 흐름을 도식화하여 (그림 1)로 나타내었다.



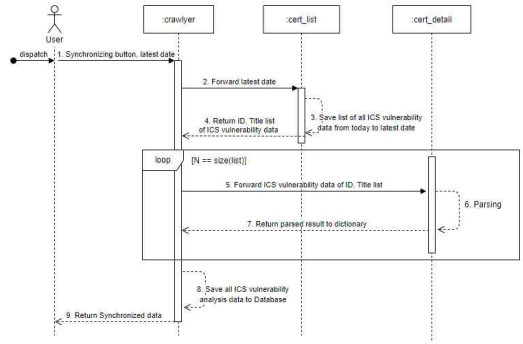
(그림 1) 프레임워크 흐름

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

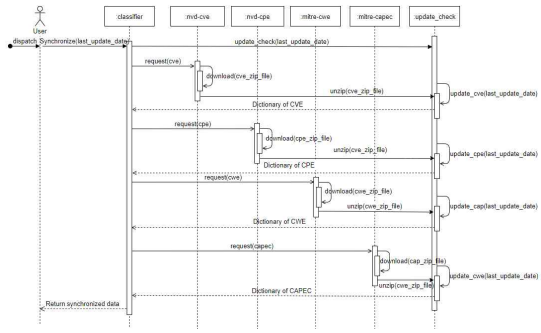
권고에는 취약점이 발생한 장비의 이름, 제조사, 영향받은 제품의 목록과 해당 취약점에 대한 CVE, CWE 등의 정보가 있다. CISA의 웹 페이지에서 모든 ICS-CERT 권고 정보를 크롤링하여 필요한 정보를 추출하고 이를 산업제어시스템 취약점 정보 데이터베이스에 저장한다. 이는 첫 번째 동기화 시점으로써 1~7일 간격으로 업데이트되는 권고 정보를 수동 및 자동으로 동기화할 수 있도록 한다. 또한, 국내 원자력 제어시스템의 특징을 반영하기 위해 국내 원자력 제어시스템의 자산 유형 정보를 추가하여 권고에서 제공하는 취약점의 자산 유형이 국내의 자산 유형에 대응될 수 있도록 하였다. 권고에서 세부적으로 다루지 않는 상용 취약점 정보인 CVE와 소프트웨어 취약점 정보인 CWE는 두 번째 동기화 시점을 통하여 공개 취약점 정보 데이터베이스를 구축하였고, 이때 CPE와 CAPEC를 배치 파일로써 저장한다.

산업제어시스템 취약점 정보와 공개 취약점 정보를 통합하여 통합 산업제어시스템 취약점 데이터베이스를 구축하여 사용자가 자산 유형을 조회했을 때 산재해 있는 ICS-CERT 권고, CVE, CWE, CPE, CAPEC에 근거한 취약점 정보를 통합적으로 조회할 수 있도록 한다.

3.2 취약점 정보원 구축



(그림 2) 산업제어시스템 취약점 정보원 구축 시퀀스 다이어그램

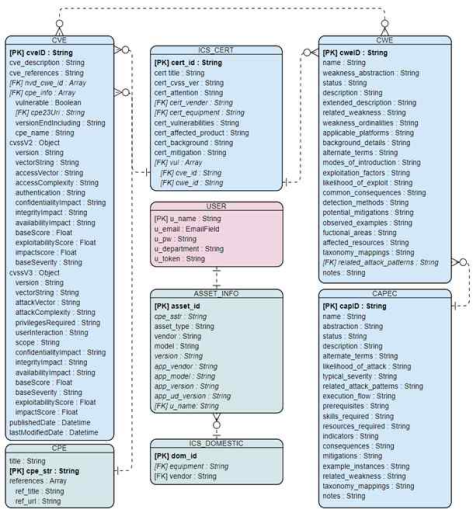


(그림 3) 공개취약점 정보원 구축 시퀀스 다이어그램

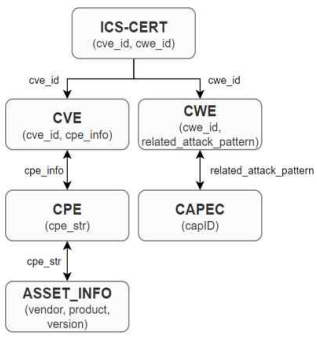
(그림 2)와 (그림 3)은 (그림 1)의 프레임워크 구축 흐름을 동기화 포인트 1과 2로 나누어 시퀀스 다이어그램을 작성한 것이다. (그림 2)는 산업제어시스템의 취약점 정보 데이터베이스 구축 및 동기화 시퀀스를 나타내며, (그림 3)은 공개 취약점 정보 데이터베이스에 대한 구축 및 동기화 시퀀스를 나타낸다.

(그림 4)는 데이터 모델링을 통해 제안하는 시스템의 구조화된 데이터를 표현한 것이다. 데이터베이스는 총 7개의 테이블을 가지며, 'ICS-CERT', 'CVE', 'CWE', 'CPE', 'CAPEC', 'ASSET_INFO', 'ICS_DOMESTIC'이 이에 해당한다.

또한 (그림 5)는 데이터베이스 테이블 간의 연관성과 속성 정보를 그림으로 나타낸 것이다. 해당 그림을 통해 각 취약점 정보 간의 관계와 외래키, CPE와 자산 정보 테이블 간의 관계성을 파악할 수 있다. 이를 통해 하나의 테이블에 속한 정보로 여러 연관된 테이블의 취약점 정보를 제공할 수 있다.



(그림 4) 개체-관계 다이어그램 (ERD)



(그림 5) 테이블 간의 연관성

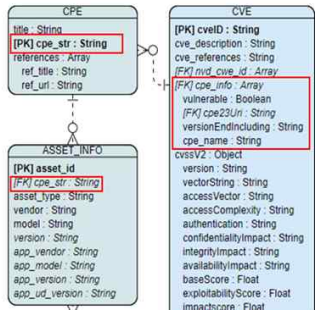
3.3 원자력 시설 자산 식별 및 취약점 분석

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 한다. 또한 취약점 검색에 사용되는 자산에 대한 정확한 식별이 필수적이다. 따라서 본 연구에서는 취약점을 검색하기 위한 CPE 기반 자산 식별 방법론을 제시한다.

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

(그림 6) CPE URI 형식

CPE는 NVD에서 발행하는 취약 자산 식별 명명 체계로, 현재 약 70만 건의 데이터가 집계되어있다. CPE는 취약한 자산에 대한 식별 정보를 URI 형식으로 제공하며, 그 형식은 (그림 6)와 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. (그림 7)과 같이 상용 취약점 정보인 CVE는 해당 취약점에 영향을 받는 자산을 'cpe_info'에 명세하고 있다.

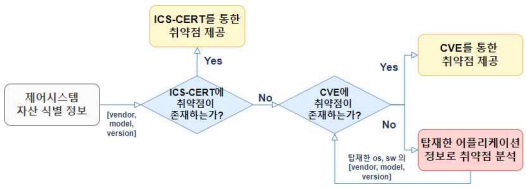


(그림 7) CPE-CVE 관계성

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 CP

E 테이블에 검색하여 대응하는 제품 리스트를 찾는다. 탐색한 제품 리스트를 드롭다운 형식으로 사용자에게 제공하여 사용자가 제품명을 고를 수 있도록 한다. 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.



(그림 8) 제어시스템 취약점 정보 분석 절차

(그림 8)은 제안하는 프레임워크가 수행하는 취약점 분석 절차이다. 이를 통해 제어시스템 자산의 제조사에 구애 받지 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. 탐색한 취약점은 자산의 잠재적인 취약점이라고 할 수 있음으로, 제안하는 취약점 탐색 방법으로 원자력 시설의 자산에 대한 취약점 검색률을 높일 수 있다.

3.4 사례 연구

<표 2>를 통해서 2가지 활용 사례를 확인할 수 있다. 첫 번째 자산인 GE의 PLC 제품은 자산의 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-CERT와 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.

4. 결론

본 연구가 제안하는 통합 취약점 분석 프레임워크는 CISA에서 제공하는 산업제어시스템 취약점 정보인 ICS-CERT를 기반으로 산재하여 있는 CVE, CWE, CPE, CAPEC 정보를 통합하였다.

<표 2> 자산 정보에 따른 취약점 정보원

자산 유형	ICS-CERT 기반 취약점 검색 속성			CPE-CVE 기반 취약점 검색 속성				취약점 정보원
	제조사	제품	버전	제조사	제품명	버전	업데이트 정보	
PLC	GE	Mark vie	*	*	*	*	*	- ICS-CERT - CVE, CWE
PLC	Soosan	POSAFE-Q	*	black berry	qnx_software_development_platform	6.4.1	*	- CVE, CWE

또한, 원자력 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.

제안하는 통합 취약점 분석 프레임워크를 이용하여 임의의 국내 원자력 시설에 대한 취약점을 분석한 결과 기존의 ICS-CERT를 통한 취약점 분석은 총자산의 8%에 대하여 취약점을 찾았지만, 제안하는 방법론은 70% 이상의 자산에 대한 취약점을 탐색하였다. 이를 국내 원자력 시설에 적용하면 자산의 제조사에 구애없이 통합적인 취약점 분석이 가능할 것으로 기대된다.

참고문헌

[1] NVD, "National Vulnerability Database", https://nvd.nist.gov/ Nov. 2021.

[2] MITRE, "CVE Data Feeds", https://cve.mitre.org/cve/data_feeds.html Nov. 2021.

[3] CISA, "ICS-CERT Advisories", https://us-cert.cisa.gov/ics/advisories Nov. 2021.

[4] KrCERT, "취약점 정보", https://www.krcert.or.kr/data/secInfoList.do Nov. 2021.

[5] NVD, "Data Feed for Vulnerabilities", https://nvd.nist.gov/vuln/data-feeds Nov. 2021

[6] NVD, "Official Common Platform Enumeration (CPE) Dictionary", https://nvd.nist.gov/products/cpe Nov. 2021.

[7] MITRE, "Common Weakness Enumeration", https://cwe.mitre.org/ Nov. 2021.

[8] MITRE, "Common Attack Pattern Enumeration and Classification", https://capec.mitre.org/ Nov. 2021.

[9] Tomas, R. J., Chothia, T. P., "Learning from Vulnerabilities - Categorising, Understanding and Detecting Weaknesses in Industrial Control Systems," CyberICPS 2020, SECPRE 2020, ADIoT 2020: Computer Security, pp. 100~116.

[10] Kim, S. W., Kim, I. K., and Kwon, K. H., "A Study on the Cyber Vulnerability Assessment of the Vital Digital Assets at the Nuclear Facilities," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 2017, pp. 725~726.

[11] Kim, M. C., Oh, S. J., and Kang, H. J., "Risk Scoring System for Software Vulnerability Using Public Vulnerability Information," Journal of the Korea Institute of Information Security & Cryptology 28(6), 2018, pp. 1449~1461.

[12] Kim, H. H., Yoo, J. H., "A Study on ICS/SCADA System Web Vulnerability," The Jounal of Society for e-Business Studies 24(2), 2019, pp 15~27.

〔저자소개〕

신 미 주 (Mi-Joo Shin)
2020년 8월 전남대학교 소프트웨어공학과 학사
2020년 9월 ~ 현재 전남대학교 정보보안협동과정 석사과정
email : shinmj8721@naver.com

윤 성 수 (Seong-Su Yoon)
2021년 2월 전남대학교 소프트웨어공학과 학사
2021년 3월 ~ 현재 전남대학교 정보보안협동과정 석사과정
email : ddorddor66@gmail.com

엄 익 채 (Ieck-chae Euom)
2003년 8월 전남대학교 컴퓨터정보학부 학사
2015년 2월 한국과학기술원 소프트웨어대학원 석사
2019년 2월 전남대학교 정보보안협동과정 박사
2019년 10월~ 현재 전남대학교 시스템보안연구센터 소장, 조교수
email : icelaken@gmail.com