Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.2, Apr. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.2.281

시계열 특성 기반의 공격자 기술 수준을 고려한 취약점 심각도 평가 방안 연구*

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

A Study on Vulnerability Severity Evaluation Considering Attacker Skill Level Based on Time Series Characteristics*

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

요 약

산업제어시스템의 특성에 대한 공격자들의 이해 증가와 더불어 정보 기술과의 연결성이 확대되면서 산업제어시스템을 대상으로 하는 보안사고가 증가하고 있다. 이와 관련된 취약점의 수는 매년 급증하고 있지만, 모든 취약점에 대해 적시의 패치를 수행하는 것은 어렵다. 현재 취약점 패치의 기준으로 여겨지는 공통 취약점 평가 체계는 취약점이 발견된 후의 무기화를 고려하고 있지않다는 한계점을 지니고 있다. 따라서 본 연구에서는 운영 기술 및 산업제어시스템 내 발생 취약점 정보가 포함된 공개 정보를 기반으로 시간의 흐름에 따라 변화하는 공격자의 기술 수준을 분류하기 위한 기준을 정의한다. 또한 해당 속성을 기존 심각도 점수 산출에 반영하여 취약점의 실제 위험성과 긴급성이 반영된 심각도를 평가하는 방안을 제안하고자 한다. 해당 평가 방안의 시계열적 특성 반영 및 운영기술 및 산업제어시스템 환경에서의 유효성을 확인하기 위해 실제 사고에 활용된 취약점에 기반한 사례연구를 수행하였다.

ABSTRACT

Industrial control systems (ICS) are increasingly targeted by security incidents as attackers' knowledge of ICS characteristics grows and their connectivity to information technology expands. Vulnerabilities related to ICS are growing rapidly, but patching all vulnerabilities in a timely manner is challenging. The common vulnerability assessment system used to patch vulnerabilities has limitations as it does not consider weaponization after discovery. To address this, this study defines criteria for classifying attacker skill levels based on open information including operating technology and vulnerability information in ICS. The study also proposes a method to evaluate vulnerability severity that reflects actual risk and urgency by incorporating the corresponding attribute in the existing severity score calculation. Case studies based on actual accidents involving vulnerabilities were conducted to confirm the effectiveness of the evaluation method in the ICS environment.

Keywords: Industrial Control System, operating technology, Ease of exploitation, Vulnerability assessment

Received(01. 05. 2023), Modified(03. 08. 2023), Accepted(03. 10. 2023)

* 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(IITP-2022-0-01203)

* 본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No. 2106061)

* 본 논문은 2022년도 한국정보보호학회 호남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임

† 주저자, ddorddor66@gmail.com

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

I. 서 론

산업제어시스템(Industrial Contol System, ICS)은 국가 중요 기반시설 설비 및 산업공정 등의 작업 공정을 감시하고 제어하는 시스템으로, 발전, 전력, 가스, 정유, 석유화학 분야 등에 널리 사용된다. 따라서, 사이버 공격에 의한 국가적인 손실을 방지하기 위해서는 취약점의 위험성 평가에 기반한 적시의 패치는 매우 중요하다.

하지만 현재의 취약점 패치 기준이 되는 공통취약점 평가체계의 기본지수 점수는 시간적인 요소를 고려하지 않기 때문에 영향 지표로 평가되는 공격 발생 후의 심각성은 평가되어도 현 시점에서의 악용될 위험성은 평가되지 않는다[1]. 시간지수 점수는 현재 각 디지털 자산의 제조사에서만 제한적으로 수행되고 있으며, 평가된 점수는 긴급성을 반영하여 증가하기보다는 기존 평가된 기본지수 점수를 감소시킨다[2].

현재 많은 보안 담당자들은 공통 취약점 평가체계의 기본지수 점수에 기반한 우선순위를 가지고 패치 관리를 직접 수행한다. 하지만 그마저도 최근에는 고위험군 이상의 취약점들 자체가 증가하다 보니 우선순위를 수립하는 것의 의미가 흐려지고 있다[3]. 이는 혼란스러운 보안 조치 우선순위를 초래하고 개선 노력을 복잡하게 만든다.

산업제어시스템은 운영 특성상, 발생한 취약점에 대한 적시의 조치가 어렵다는 한계가 존재한다. 이로 인해 시간의 흐름에 따라 변화하는 공격자의 기술 수준을 반영한 취약점 심각도를 평가하여 사전에 발생할 수 있는 잠재적인 취약점을 방어하는 것이 필요하다.

따라서 본 논문에서는 시계열 특성 기반의 공격자 기술 수준을 고려한 취약점 심각도 평가 방안에 관한 연구를 수행하였다. 시계열적 특성을 지닌 공격자의 기술 수준 정보를 내포한 취약점 속성을 활용하여 패치 우선순위의 기준이 되는 기본지수 점수 산출에 실제 악용 위험성을 내포하도록 하였으며, 이를 통해 긴급성이 반영된 취약점 패치가 가능하도록 하였다. 공개된 취약점 및 익스플로잇(exploit) 정보를 기반으로 분류 기준을 정의하여 기존의 제조사 등에 한정된 시계열적 특성을 지닌 공격자의 기술 수준 평가를 일반화하였다. 해당 속성을 취약점 심각도 점수 산출에 반영하여 점수를 증가시켰으며, 이는 기존의 시간적 요소 적용시 점수가 감소하던 한계점을 개선하였다. 운영기술 및 산업제어시스템에 대한 APT 공격 정보를 활용한 공격자의 기술 수준 평가를 통해 특정 운영 환경 특성 및 시간의 흐름에 따른 취약점 악용 위험성 평가가 가능하도록 하였다. 제안하는 평가방안을 실제 발생한 사이버 사고에 적용한 사례연구를 수행하여 실제 악용 위험성이 반영된 패치 전략 수립이 가능함을 확인할 수 있도록 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 취약점 심각도 평가에 대한 연구에 관해 기술한다. 3장에서는 시계열 특성 기반의 공격자 기술 수준 평가를 위한 속성 및 평가 분류 기준 정의하고, 이를 활용한 취약점 심각도 정량화 방안을 제시한다. 4장은 제안된 평가 방안을 실제 사이버 사고에 적용하여 평가를 수행하며, 평가 결과를 분석한다. 마지막으로 5장에서 결론을 내리며 마무리한다.

II. 관련 연구

2.1 취약점 평가 체계 및 보안 평가 방법론

2.1.1 공통 취약점 평가체계 (Common Vulnerability Scoring System, CVSS)

CVSS[4]는 취약점의 영향과 특징을 전달하기 위한 오픈 프레임워크를 제공하고 있다. 취약점의 정적 속성 정보를 나타내는 기본지수(base metric), 시간의 흐름에 따라 변화하는 취약점의 특성을 나타내는 시간지수(temporal metric), 사용자 환경을 고려한 취약점의 특성을 나타내는 환경지수(environment metric)로 3가지 평가 그룹을 정의하고 있다.

CVSS의 점수 산출 방식은 Fig. 1.과 같은 구조로 기본 점수에 대해 악용 가능성(exploitability), 영향도(impact), 범위(scope)에 따라 0부터 10까지 위험도를 산출하며, 목적에 따라 시간 점수, 환경 점수 산출 식을 포함하여 취약점 심각도 점수를 계산할 수 있다.

CVSS는 최초 발표된 이 후, 2019년까지 정량적

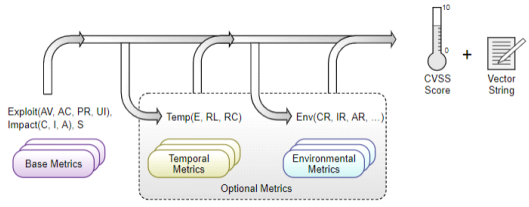

Fig. 1. CVSS scoring method

인 위험 평가 체계 수립을 위해 새로운 평가 항목을 도입하거나 기존 평가 항목을 개선하며 발전하였다. 이 중, 기본 지수의 '공격 복잡도(attack complexity)'는 버전 1.0에서 공격을 수행하기 위한 전제 조건과 더불어 공격자의 기술 수준을 파악하여 평가하였으나, 버전 3.1에서는 공격자의 기술 수준을 분리하여 평가를 수행하고 있다.

공격자의 기술 수준을 나타내는 공격 코드의 유무는 사이버 공격을 수행함에 있어 악용을 용이하게 하기때문에, 본 연구에서는 기본 지수에서의 부가적인 평가 요소로써 악용 용이성 판단을 위해 CVSS 버전 1.0의 공격 복잡도 평가 관점을 적용하였다. 해당 항목의 버전별 고려사항은 다음 Table 1.과 같다.

Table 1. Attack complexity considerations by CVSS version

Version	Considerations	
	Prerequisites before performing an attack	Attacker's skill level
1.0		●
2.0	●	
3.0	●	
3.1	●	

2.1.2 발전시설 대상 사이버 보안 평가 방법론 (Technical Assessment Methodology, TAM)

TAM[5,6]은 발전시설의 잠재적인 위협 요소를 고려하여 사이버 보안 조치를 식별하고, 식별한 사이버보안 조치의 효과성과 적합성을 정량화하여 사이버 보안 조치의 성능을 평가할 수 있는 미국 전력연구원(Electric Power Research Institute, EPRI)에서 개발한 방법론이다.

Fig. 2.는 TAM의 보안 조치 평가를 위한 3단계 절차를 나타낸 그림이다. TAM은 해당 절차를 지나며, 취약점 악용 난이도를 설정함에 있어 CVSS를 활용한다. 여기서 CVSS의 취약점의 정적 특성을 나타내는 기본 지수 점수의 악용 가능성 지수와 취약점의 동적 특성을 나타내는 시간 지수 점수는 악용 난이도를 설정하는데 기반이 된다. 또한 TAM은 악용 난이도를 설정하기 위해 기존 CVSS 평가 항목의 정의를 개선하여 적용해야함을 강조한다. 특히, 기본

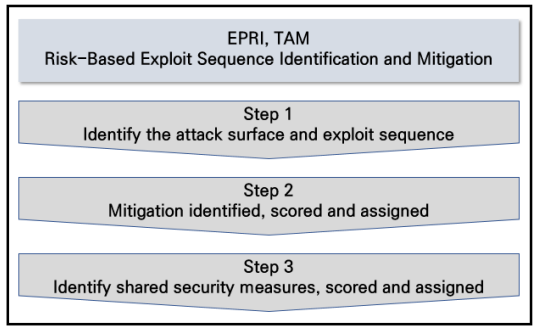

Fig. 2. EPRI's TAM Schematic Diagram

지수 점수의 평가 항목인 '공격 복잡도'는 기존의 '공격자가 공격을 수행하기 위해 전제되어야 하는 조건' 외 시간에 따라 변화하는 '공격자의 기술 수준'을 함께 포함하였다.

2.2 취약점 심각도 평가 관련 연구 분석

공개된 취약점 정보 및 익스플로잇 정보를 활용하여 공격자의 기술 수준을 평가하는 연구들이 수행되었다. 해당하는 연구들로는 공격자의 기술 수준을 평가하기 위해 CVSS의 시간 지수 평가를 활용하는 연구와 기존에 없던 새로운 평가 속성을 추가하고, 이를 점수 산출에 반영하여 평가를 수행하는 연구가 존재한다.

Jung. B 등[7]은 취약점의 무기화 수준 정보를 반영하기 위해 CVSS의 시간 지수 평가 속성 중 '공격 코드 성숙도'를 공개된 취약점의 참조 URL 및 태그 정보를 활용하여 평가 기준을 정의하였다. 이를 기반으로 시간 지수 평가를 자동화하고, 평가된 점수에 따른 패치 우선순위를 지정함으로써 취약점이 현재 얼마나 악용되기 쉬운지에 대한 컨텍스트 정보를 활용하고자 하였다. 하지만 평가된 시간 지수 점수가 여전히 심각도 점수를 낮추고 있을 뿐, 취약점의 무기화 수준을 추적하고, 이후 점수를 높이는 데 필요한 기능을 제공하지 않고 있다는 한계점이 존재한다.

Singh. U. K 등[8]은 취약점 정보로부터 얻어진 공격코드 성숙도와 패치 수준 정보를 활용하여 CVSS의 시간 지수 점수를 산출하고, 산출한 시간 지수 점수와 CVSS 기본 지수 속성 정보를 활용하여 악용 빈도를 계산하였다. 이에 더해 최종 산출된 악용 빈도를 CVSS 심각도 산출의 가중요소로 적용하여 정량적인 보안 위험 수준을 추정하였다. 그러나 해당 평가를 위한 기본 속성인 공격코드 성숙도의 판

단 기준이 표준화되어 있지 않으며, 주로 경험적인 판단에 근거하고 있다.

Bulut 등[9]은 취약점의 악용 용이성을 판단하기 위해 'Weaponized Exploit(WX)', 'Utility', 'Opportune'의 3가지 새로운 속성을 정의하였다. 이를 평가하기 위해 Exploit DB, Metasploit, github에서 언급되는 참조 링크의 총개수와 전문가의 판단 정보를 활용하였다. 또한 이를 기존 CVSS 심각도 점수 산출의 추가적인 가중요소로 적용해 0~10점으로 산출되던 심각도 값을 25~453 사이의 값으로 산출하였다. 하지만 전문가의 경험적인 판단에 의존하고 있어 일관된 평가가 어렵다는 한계점과 산출된 위험 점수의 정량적 수치에 대한 판단 기준이 명확하지 않아 적시의 취약점 무기화 수준 및 악용의 용이성 판단이 어렵다는 한계점이 존재한다.

Farris 등[10]은 기존의 CVSS가 실제 위험성을 나타내는 데 한계가 있다는 문제를 해결하기 위해 취약점 복구 시간 및 노출된 취약점 두 가지 요구사항 지표를 활용하여 취약점 관리 전략 프레임워크인 VULCON(VULnerability CONtrol)을 제안하였다. 하지만 해당 연구는 관리적인 측면에 초점이 맞춰진 연구로써 본 연구에서 논의하고자 하는 공격자의 기술 수준 및 공격 코드의 무기화 수준을 평가하는 데에 있어 차이점이 존재한다.

또한 기존에 수행된 연구들은 공통적으로 본 연구에서 고려하고자 한 시간의 흐름에 따른 공격자의 기술 수준 파악 외, 운영기술(Operational Technology, OT) 및 산업제어시스템 환경에서 발생한 취약점의 위험성을 고려하지 않고 있다는 한계점이 존재한다. Table 2.는 관련 연구에 대하여 비교 분석한 결과를 반영된 연구 특성 기준으로 분류한 표이다.

Table 2. Characteristics of studies related to vulnerability exploitability evaluation

Paper	Evaluation Attribute		Domain		
	weaponization level	patch level	IT	OT	ICS
[7]	●		●		
[8]	●	●	●		
[9]	●		●		
[10]		●	●		

III. 시계열 특성을 반영한 공격자 관점의 취약점 심각도 평가 방안

본 연구에서는 CVSS와 기존 관련 연구의 한계점을 보완하여 시간의 흐름에 따른 실제 위험성이 반영된 취약점 심각도를 평가하기 위해 Fig. 3.과 같은 평가 방안을 제안한다.

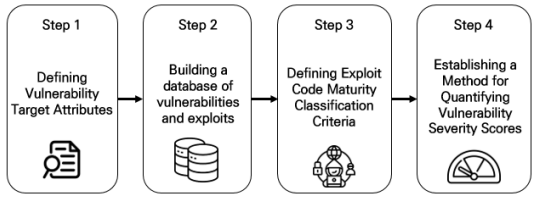

Fig. 3. Procedures for Conducting Vulnerability Severity Assessment Studies

3.1 취약점의 시계열 특성 반영된 평가 속성 정의

현재의 CVSS는 앞서 논의한 바와 같이 심각도는 측정되어도 실제 공격 수행 위험성 및 긴급성은 반영하지 못한다는 한계점과 향후의 위협 수준 예측을 위한 무기화 정보 제공이 어렵다는 한계점이 존재한다. 또한 시간 지수 각 속성에 대한 명확한 평가 기준이 존재하지 않아 제조사의 자체적인 평가로 제한되어 있으며, 평가된 시간지수 점수가 기존의 평가 점수를 낮출 뿐이라는 한계점이 존재한다.

이를 위해서는 실제 공격자나 침투 테스터가 공격을 수행할 시 활용할 공격 기술 및 취약점의 무기화 수준 정보가 고려된 악용 용이성을 반영해야 하며, 공개된 익스플로잇 정보를 기반으로 한 일반화된 시간지수 평가가 수행되어야 한다.

본 연구에서는 이를 바탕으로 취약점 심각도 평가 시, 시간이 지남에 따라 변화하는 '공격자의 기술 수준'을 반영한 악용 용이성 평가를 수행하여 기본지수 평가에 반영하고자 한다. 이를 위해 CVSS의 시간지수 평가 속성 중 공격에 활용될 익스플로잇에 대한 가용 수준을 의미하는 '공격코드 성숙도'를 평가 속성으로 선정한다.

공격코드 성숙도의 평가 지표는 '정의되지 않음(Not Defined)', '검증되지 않음(Unproven)', '개념증명(Proof of Concept)', '무기화된 공격코드(Functional)', '자동화된 공격코드(High)'로 이루어져있으며, 해당 속성은 시간이 지나 익스플로잇이

공개되거나 자동화되면서 수준이 점차 변화한다.

해당 속성은 기존 시간지수 평가의 한계점을 동일하게 지니고 있으며, 이를 해결하기 위한 방안을 적용하여 분류 기준 정의 및 정량화 방안을 도출한다.

3.2 취약점·Exploit 데이터베이스 생성

시계열 특성이 반영된 취약점 심각도 평가와 운영기술 및 산업제어시스템 환경에서 발생하는 취약점에 적용할 수 있는 평가 방안을 활용하기 위해 공개된 취약점 정보와 익스플로잇 정보를 수집하여 데이터베이스를 생성한다.

3.2.1 취약점 데이터베이스

본 연구에서 활용되는 취약점 정보원은 NVD(National Vulnerability Database)에서 제공되는 상용 취약점 정보(Common Vulnerabilities and Exposures, CVE)[11]와 취약 자산 식별 명명 체계(Common Platform Enumeration, CPE)[12]가 있으며, MITRE에서 제공되는 소프트웨어 취약점 정보(Common Weakness Enumeration, CWE)[13]와 공격 패턴 정보(Common Attack Pattern Enumeration and Classification, CAPEC)[14]이 있다. 운영기술 및 산업제어시스템 환경에서 발생한 취약점에 대한 표준화된 정보원으로는 CISA (Cyber security and InfrastructureSecurity Agency)에서 제공하는 ICS-CERT 권고(Advisories)[15]가 있으며, 이를 통해 운영기술 및 산업제어시스템 환경에서 발생하는 취약점 유형을 파악하고, 이를 고려한 평가 방안 수립이 가능하다.

3.2.2 Exploit 데이터베이스

취약점 정보 외에 시간의 흐름에 따른 공격코드 성숙도 분류 및 운영기술 및 산업제어시스템 환경을 고려한 심각도 평가를 위해 악용 정보 수준 별 공개된 최신화 익스플로잇 정보를 수집하였다. 본 연구에서 수집된 PoC(Proof of Concept) 수준의 정보는 기존 연구에서도 활용된 Exploit-DB[16]와 Github[17]가 있다. Functional 수준의 정보로는 실제 악용된 취약점 정보를 제공하는 CISA의 알려진 악용된 취약점 정보(Known Exploited Vulnerability, KEV)[18]와 지능형 지속 공격(Advanced Persistent Threat, APT) 그룹 등 국가 차원의 기반 시설에서 발생한 보안 문제, 취약성 및 악용에 대한 정보를 제공하는 국가 사이버 인식 시스템 경고 정보(National Cyber Awareness System, NCAS)[19]가 있다. 마지막으로 High 수준의 정보로는 취약점에 대한 자동화된 공격 모듈 정보를 제공하는 Rapid7의 Metasploit[20]이 있다.

3.2.3 취약점·익스플로잇 데이터 연관성

Fig. 4.는 구축한 데이터베이스 테이블 간의 연관성과 관련 속성 정보를 그림으로 나타낸 것이다. 보이는 바처럼 각 취약점 정보는 특정 속성 정보를 기반으로 연관성을 지니고 있으며, 익스플로잇 정보는 원천 취약점 정보인 CVE 식별자를 기반으로 취약점 정보와의 연관성을 지닌다. 이와 같은 연관성 정보를 기반으로 취약점의 무기화 수준을 파악할 수 있다.

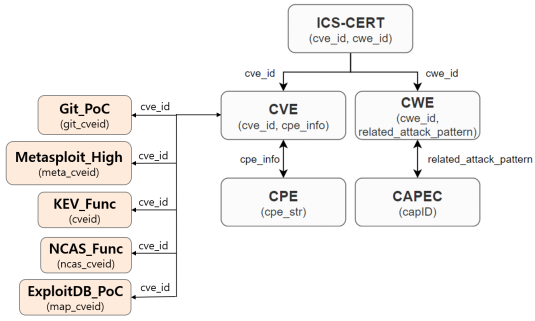

Fig. 4. Correlation between vulnerability and Exploit information

3.3 공격코드 성숙도 분류 기준 정의

기존 CVSS 시간 지수의 평가 속성인 공격코드 성숙도는 표준화된 분류 기준 없이, 각 조직의 자체적인 분류 기준을 기반으로 분류를 수행해왔다. 이에 관하여 본 연구에서는 취약점 정보원과 익스플로잇 정보원의 공개된 데이터에 기반하여 평가 대상 속성으로 정의된 공격 코드 성숙도에 대한 분류 기준을 정의하였다. 다음 Fig. 5.는 두 가지 세부 분류 기준을 통합하여 구현한 전체적인 공격코드 성숙도 분류 절차이다.

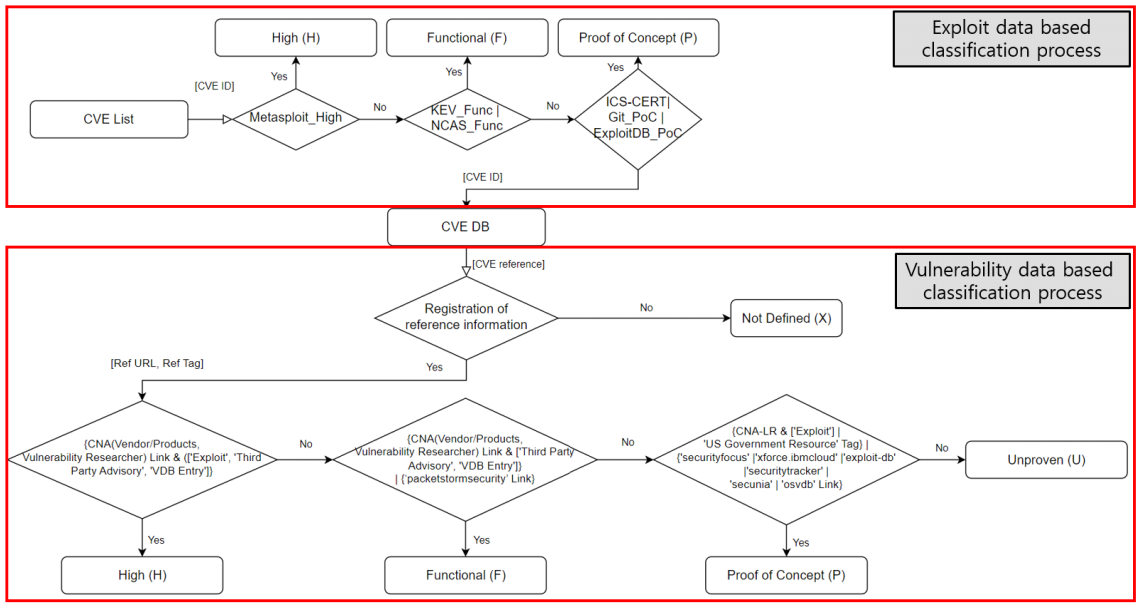

Fig. 5. Exploit Code Maturity Classification Process

3.3.1 익스플로잇 정보원 기반 분류 기준 정의

익스플로잇 정보원을 기반으로 하는 공격 코드 성숙도 분류 기준은 수집된 익스플로잇 정보에서 제공되는 취약점 무기화 수준 정보에 따라 정의되었다.

모의해킹을 위한 자동화 모듈을 제공하는 Metasploit에 포함된 CVE 정보는 공격 코드 성숙도의 지표 중 'High'로 분류되며, 실제 환경에서 사이버 공격에 악용된 취약점 정보를 제공하는 CISA의 KEV와 NCAS에 포함된 CVE 정보는 공격 코드 성숙도의 지표 중 'Functional'로 분류된다. 다음으로 공격의 실현 가능성을 검증하기 위한 PoC 정보를 제공하는 Exploit-DB 및 Github에 포함된 CVE는 공격 코드 성숙도의 지표 중 'Proof of Concept'로 분류된다.

또한 본 연구에서는 시스템에 영향을 미치지 않더라도 취약점으로 인한 영향성이 발견되는 것 자체로 위험하다는 산업제어시스템 운영 특성에 기반하여 ICS-CERT 정보를 'Proof of Concept' 분류 기준에 포함하였다. Table 3.은 정의된 익스플로잇 정보원 기반 분류 기준이다.

Table 3. Classification Criteria Based on Exploit Sources

Exploit Code Maturity	Classification Criteria
High	{Metasploit}
Functional	{KEV | NCAS}
PoC	{ExploitDB | Github | ICS-CERT}

3.3.2 취약점 정보 기반 분류 기준 정의

취약점 정보를 기반으로 하는 분류 기준은 익스플로잇 정보원에 대한 연결 정보가 존재하지 않는 CVE 또는 신규 발견된 CVE에 대한 공격 코드 성숙도를 분류하기 하기 위해 정의하였다. 이를 위해 CVE 참조 정보를 구성하는 URL과 태그 정보에 대하여 CVE-Exploit 정보원의 연관 분석을 수행하였다.

해당되는 참조 정보는 'cve_references' 필드 정보가 기반이 되었으며, 해당 필드 정보에는 취약점에 대한 권고 사항, 패치 정보, 악용 정보, 분석 보고서 등이 포함된 URL이 제공되고, 각 참조 정보가 포함하는 내용에 대한 태그(tag) 정보가 제공된다. 분석 정보로 활용된 참조 URL은 전체 CVE 195,581개에 포함된 13,307개이며, 이에 대한 태그 정보는 총 18개로 이루어져있다.

분류 기준 정의를 위한 CVE-Exploit 연관 분석은 공격코드 성숙도 별 익스플로잇 정보와 매핑되는 CVE에 포함된 URL, 태그 발견 빈도와 전체 CVE

에서 발견된 URL, 태그 빈도에 대한 통계 분석을 통해 수행되었다. 사용된 공격코드 성숙도 별 익스플로잇 정보가 존재하는 CVE는 PoC 수준 26,329개, Functional 수준 2,658개, High 수준 4,236개이다.

연관 분석 중, URL 정보 통계 분석은 공격코드 성숙도 별 익스플로잇 정보와 매핑되는 CVE에 포함된 URL 정보를 기반으로 수행된다. 각 수준에서 추출된 URL 정보는 해당되는 공격코드 성숙도 CVE 그룹에서의 발견 빈도를 측정한다. 각 수준에서 측정된 URL 발견 빈도와 전체 CVE 내에서의 URL 발견 빈도를 비교하여 해당되는 공격코드 성숙도 정보 제공 확률을 25%, 50%의 범위로 측정하였다.

다음으로 태그 정보 통계 분석은 독립된 태그 외에 태그 조합에 대한 분석을 함께 수행한다. 공격코드 성숙도 별로 익스플로잇 정보와 매핑되는 CVE에 포함된 태그 및 태그 조합을 추출한다. 그 다음 각 수준에 해당하는 CVE에 대하여 해당 태그 및 태그 조합 발견 빈도를 측정한다. Fig. 6.은 차례대로 PoC, Functional, High 수준에서의 URL, 독립된 태그, 태그 조합 분석 결과를 나타낸다.

해당 URL 분석 결과를 통해 각 수준 별 25% 이상의 확률로 무기화 정보를 제공하는 URL에 대하여 중복 제거한 후 분류 기준으로 선정하였다. 태그 분석 정보 결과로부터는 각 수준 별 발견 빈도 상위의 독립된 태그 및 태그 조합을 분류 기준으로 선정하였다. 또한 공통된 상위 태그 및 태그 조합인 'Vendor Advisory', 'Third Party Advisory'에 대한 분류를 위해 CVE 식별자 할당 기관(CVE Numbering Authority, CNA)[21]과의 연결 정보를 기반으로 추가적인 URL 분류 기준을 선정하였다.

이에 더해 운영기술 및 산업제어시스템 환경을 고려한 분류 기준 정의를 위해 PoC 수준 CVE에서 유일하게 상위 태그로 선정된 'US Government Resource'에 연결되는 URL 정보로써 산업제어시스템 및 의료 장비와 같은 기존 CNA 역할의 범위 속하지 않는 분야의 취약점에 대한 CVE 식별자를 할당하는 CNA-LR(CVE Numbering Authority of Last Resort)[21] 기관의 URL 정보를 분류 기준으로 추가 선정하였다. Table 4.는 최종 정의된 취약점 정보 기반 분류 기준이다.

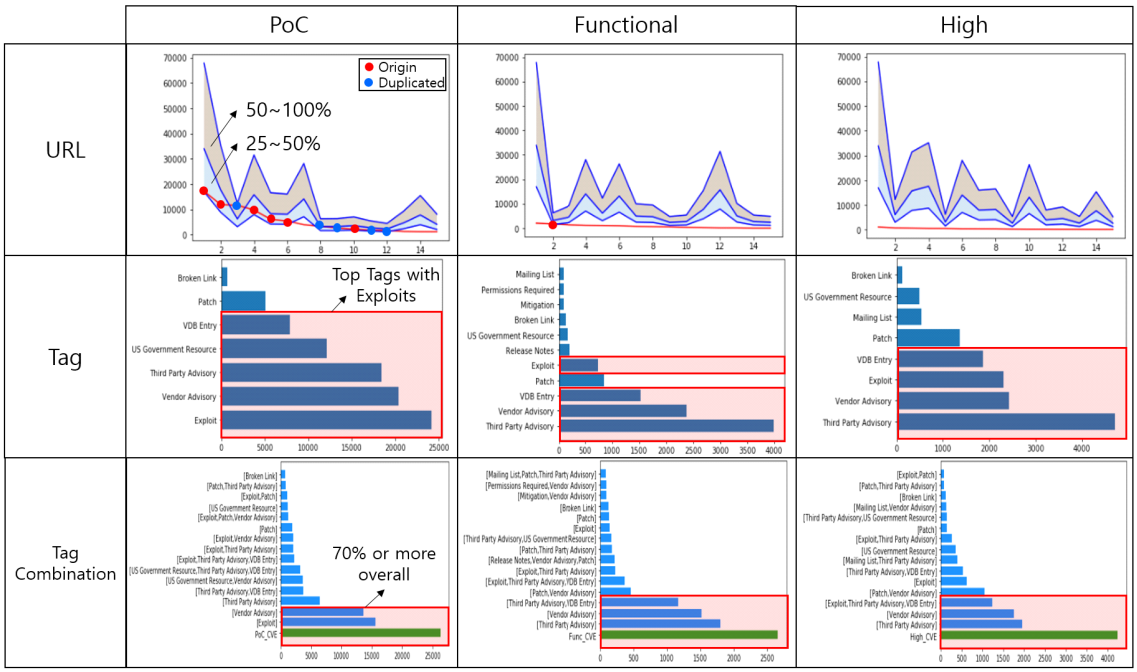

Fig. 6. Results of URL, independent tag, and tag combination analysis by weaponization information level

Table 4. Classification criteria based on vulnerability information

Exploit Code Maturity	Classification Criteria
High	{CNA(Vendor/Products, Vulnerability Researcher) Link & ({'Exploit', 'Third Party Advisory', 'VDB Entry'} Tag)}
Functional	{CNA(Vendor/Products, Vulnerability Researcher) Link & {'Third Party Advisory', 'VDB Entry'}} | {'packetstormsecurity' Link}
PoC	{CNA-LR & ({'Exploit'} | 'US Government Resource' Tag)} | {'securityfocus' |'xforce.ibmcloud' |'exploit-db' |'securitytracker' | 'secunia.com'| 'osvdb.org' Link}
Unproven	Not satisfy any rules above
Undefined	Unable to obtain information

3.4 취약점 심각도 정량화

CVSS에서 공개된 공격코드 성숙도에 대한 각 지표와 가중치는 다음 Table 5.와 같다. 해당 가중치는 기존 CVSS 시간지수 점수 평가 시, 산출된 기본지수 점수보다 낮아진 점수를 산출하여 정확한 악용 위험성을 판단하기가 어렵게 한다.

본 연구에서는 '공격자의 기술 수준' 정보를 제공하는 공격코드 성숙도를 기본지수 점수 산출에 적용하여 전체 심각도 점수를 증가시키고, 최종적으로 취약점에 대한 시간의 흐름에 따른 위험성과 긴급성이 반영된 점수를 산출하고자 한다. 이를 위해 '공격자가 공격을 수행하기 위해 전제되어야 하는 조건'인 공격 복잡도와 공격코드 성숙도를 결합하여 '공격이 얼마나 용이하게 수행될 수 있는지'를 의미하는 '악용 용이성'을 정량화한다. 그 다음, 정량화된 '악용 용이성'을 기본 지수 산출식의 가중 요소로 더하여 0~10 사이의 점수를 산출하도록 한다. Table 6.은 본 연구에서 CVSS의 기본지수 점수 산출식을 기반으로 수정한 악용 용이성이 반영된 취약점 심각도를 정량화하는 산출식을 나타낸 것이다.

이는 기존 CVSS의 시간 지수 점수 산출 시 점수가 감소하는 한계점을 보완하고, 각 수준에 따라 심각도 점수가 증가하게 되어 실제적인 취약점의 위험성 및 긴급성에 대한 정보를 제공할 수 있다. 또한 기존 취약점의 정적인 특성만을 기반으로 심각도를 계산했던 기본 점수에 시간의 흐름에 따라 변화하는 익스플로잇의 가용 수준 정보를 고려하여 취약점의 정적, 동적 특성이 모두 반영된 종합적인 심각도 점수를 산출할 수 있다.

Table 5. Indicators and Weights of Exploit Code Maturity

Classification Indicator	Weight
Undefined (X)	1
Unproven (U)	0.91
Proof of Concept (P)	0.94
Functional (F)	0.97
High (H)	1

Table 6. Severity score calculation formula reflecting attack code maturity

ISS =	$1-[(1-Confidentiality)\times(1-Integrity)\times(1-Availability)]$
Impact =	
If Scope is Unchanged	$6.42\times ISS$
If Scope is Changed	$7.52\times(ISS-0.029)-3.25\times(ISS-0.02)^{15}$
Exploitability =	$8.22\times AttackVector\times AttackComplexity\times PrivilegesRequired\times UserInteraction$
EaseOfExploitation =	$AttackComplexity\times ExploitCodeMaturity$
BaseScore =	
If Impact <= 0	$0,\ else$
If Scope is Unchanged	$Roundup(Minimum[(Impact+Exploitability+EaseOfExploit),10])$
If Scope is Changed	$Roundup(Minimum[1.08\times(Impact+Exploitability+EaseOfExploit),10])$

IV. 사례 분석

4.1 시계열 특성 반영된 취약점 심각도 평가

본 연구에서 선정한 '공격코드 성숙도' 속성이 가지는 시계열 특성을 확인하고자 실제 공격에 수행되어진 취약점 가지고, 사례 연구를 수행하였다. 평가를 위해 선정된 취약점은 2021년 6월에 등록된 'CVE-2021-1675'이다. 해당 취약점 정보는 2022년 7월 2일까지 총 7번에 걸쳐 변경이 된 것으로 확인되었다. 공격코드 성숙도를 고려한 취약점 악용 가능성 평가 시, 시간의 흐름에 따라 점수의 변동을 보기 위해 Table 7.과 같이 7번의 변경 날짜와 익스플로잇 정보원 등록 날짜에 기반해 10개의 날짜에 대하여 점수 산출을 수행하였다.

취약점 변경 및 Exploit 정보원 등록 시간축 별로 본 연구의 평가 방안을 적용해본 결과 Exploit 관련 정보가 시간이 흐름에 따라 추가되면서, Fig. 7.과 같이 해당 취약점의 기존 CVSS 심각도 점수는 8.8점의 High에 머무르는 반면, 21년 7월 7일 이후로 9.4점의 Critical로 변경된다. 해당 점수는 공격이 성공할 시, 미치는 영향이 치명적일뿐만 아니라, 현재 악용에 사용되는 공격자의 기술 수준이 안정화되어 있음을 의미한다.

실제 해당 취약점은 2022년 9월 6일 캘리포니아주 최대 공립학교 시스템인 로스앤젤레스 통합 학구의 교육기관을 대상으로 한 랜섬웨어(ransomware) 공격에서 활용되었다. 만약 본 연구에서 수행한 평가 방안을 적용했다면 기존 취약점의 심각도에 공격자의 무기화 수준이 고려되어 그 위험성과 긴급성이 반영된 점수가 산출되었을 것이다.

Table 7. CVE-2021-1675 Information Change History and Exploit Information Source Registration History

Date	Exploit Code Maturity	Existed Score	Suggested Score
21.6.8	X	0	0
21.6.10	X	7.8	7.8
21.6.27	P	7.8	8.1
21.7.1	P	7.8	8.1
21.7.2	P	7.8	8.1
21.7.5	F	7.8	8.4
21.7.7	F	8.8	9.4
22.5.24	H	8.8	9.6
22.5.25	H	8.8	9.6
22.7.2	H	8.8	9.6

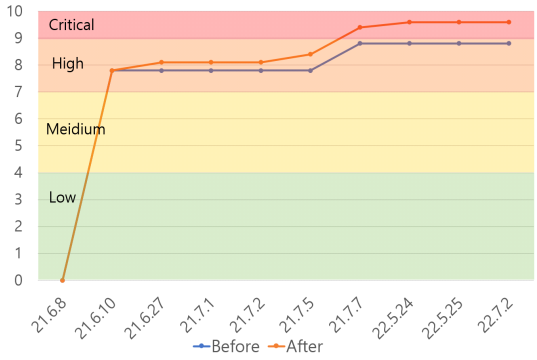

Fig. 7. 'CVE-2021-1675' score change before and after reflection of attack code maturity

이를 통해 취약점의 무기화 정보를 지속적으로 추적할 수 있었을 것이며, 실제 환경에서 점수가 Critical로 변경되었을 21년 7월에 그 긴급성과 위험성이 반영되어 보안 조치가 우선적으로 수행되었을 것이다.

결과적으로 시간이 지남에 따라 변경되는 공격코드 성숙도로 점수가 증가함으로 인해 해당 속성이 취약점 악용 가능성 평가에 있어 시계열적인 특성을 지니고 있음을 발견할 수 있다.

4.2 운영기술 및 산업제어시스템 대상 사이버 사고 악용 취약점 평가 적용 사례

4.2.1 Shammon V3 공격

Shamoon은 중동 및 남부 유럽의 석유, 가스, 에너지 산업을 타겟으로 하는 2012년에 처음 등장한 맬웨어이며, 버전 별로 기능을 공유하거나 업데이트하여 2018년에 발견된 버전 3은 시스템을 감염시키는 즉시 파괴적인 작업을 수행할 수 있다는 특징을 지니고 있다. Shamoon V3 공격은 APT33 및 Elfin으로 알려진 이란 기반 해킹 그룹에 의해 수행되었다.

대표적인 사이버 사고로는 2018년에 이탈리아 석유 및 가스 회사인 Saipem에 대하여 수행된 공격이 있다. 해당 공격에 사용된 취약점 중 권한 상승의 목적으로 악용 타겟이 된 취약점으로 CVE-2017-0213이 있는데, 이는 Windows에 존

재하는 Windows COM Aggregate Marshaler의 권한 상승 취약성을 악용한다.

해당 취약점은 실제 산업제어시스템에 대한 파괴적인 공격에 활용되었음에도 불구하고 최초 Microsoft 社에서 보고한 CVSS 심각도 점수인 6.7점으로 MEDIUM 수준의 심각도를 나타내고 있으며, 여전히 보안 조치 대상 취약점으로 중요시 여겨지지 않고 있다. 이에 본 연구에서 제안하는 공격코드 성숙도를 고려한 악용 가능성 평가를 해당 취약점에 적용한 결과 CISA의 KEV와 NCAS에 존재하여 공격코드 성숙도가 'Functional'로 분류되었고, 심각도 점수는 7.1점의 심각도 HIGH로 평가되었다.

이로 인해 기존 CVSS에서는 보안 조치 대상에서 제외되었던 우선순위가 공격코드 성숙도를 고려한 평가를 통해 실제 악용에 사용되어질 가능성이 높다고 평가되면서 새롭게 보안 조치 대상에 포함되었다. Fig. 8.은 실제 구현된 프로세스에 의해 출력된 결과이며, Fig. 9.는 심각도 점수 비교 그래프이다.

```
Vulnerability : CVE-2017-0213
-------Before reflecting attack code maturity---------
Severity Score : 6.7
CVSS Vector : CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
-------After reflecting attack code maturity----------
Severity Score : 7.1
CVSS Vector : CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/ECM:F
```

Fig. 8. Results output by the actual implemented process for CVE-2017-0213

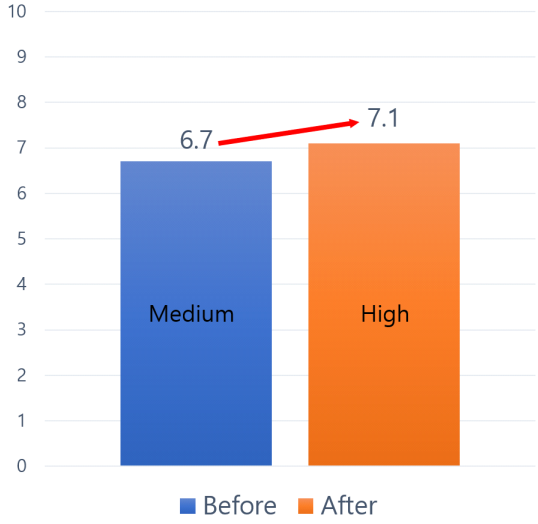

Fig. 9. Comparison of severity scores for CVE-2017-0213

4.2.2 Ryuk 랜섬웨어

Ryuk 랜섬웨어는 돈을 지불할 가능성이 가장 높은 의료 기관과 같은 취약한 기관을 대상으로 하는 2018년에 등장한 자가 복제 랜섬웨어이다. Ryuk 랜섬웨어 공격은 러시아 기반 해킹 그룹으로 알려진 WIZARD SPIDER의 하위 그룹인 GRIM SPIDER에 의해 수행되어왔으며, COVID 기간 동안 공격이 급증하여 2020년 의료에 대한 모든 사이버 공격의 1/3을 수행하였다.

해당 랜섬웨어 공격에 사용된 취약점은 2017년부터 2019년 중반까지의 오래된 취약점들이었으며, 이 중 초기 접근 및 권한 상승의 목적으로 악용 대상이 된 취약점 중 하나로 CVE-2019-6109가 있다.

해당 취약점은 실제 공격에 활용되었음에도 불구하고 최초 등록된 CVSS 심각도 점수인 6.8점으로 'MEDIUM' 수준의 심각도를 나타내고 있으며, 여

```
Vulnerability : CVE-2019-6109
-------Before reflecting attack code maturity---------
Severity Score : 6.8
CVSS Vector : CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N
-------After reflecting attack code maturity----------
Severity Score : 7.3
CVSS Vector : CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N/ECM:F
```

Fig. 10. Results output by the actual implemented process for CVE-2019-6109

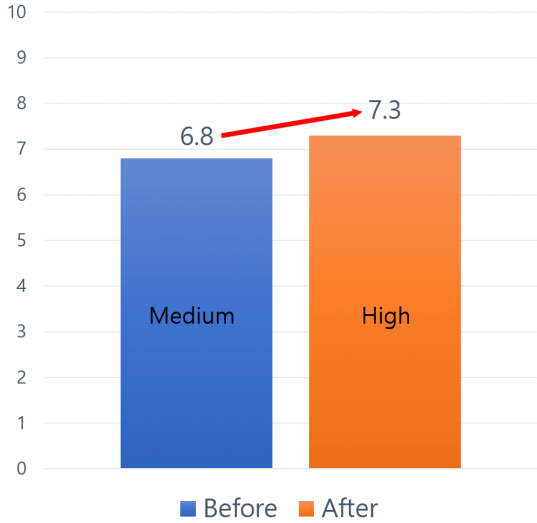

Fig. 11. Comparison of severity scores for CVE-2019-6109

전히 보안 조치 대상 취약점으로 중요시 여겨지지 않고 있다. 이에 본 연구에서 제안하는 공격코드 성숙도를 고려한 악용 가능성 평가를 해당 취약점에 적용한 결과 CISA의 NCAS에 존재하여 공격코드 성숙도가 'Functional'로 분류되었고, 심각도 점수는 7.3점의 심각도 HIGH로 평가되었다. Fig. 10.은 실제 구현된 프로세스에 의해 출력된 결과이며, Fig. 11.은 심각도 점수 비교 그래프이다.

4.2.3 사이버 사고 악용 취약점 평가 결과 토의

평가 결과를 통해 해당 취약점이 실제 APT 그룹이나 랜섬웨어 공격에 대한 정보를 제공하는 익스플로잇 정보원에 연결이 되면서 정보 기술(Information Technology, IT) 분야가 아닌 운영 기술 및 산업제어시스템 환경에서 발생한 취약점에 대해서도 공격코드 성숙도 평가가 가능함을 발견할 수 있다.

또한 두 사례에서 발견할 수 있듯이 기존 7.0 이하의 보안 조치 대상이 아니었던 취약점의 점수가 증가하면서 방어자로 하여금 동일 점수대의 수많은 취약점 중에서 실제 악용될 위험이 높은 취약점에 대하여 우선순위 선정이 가능하도록 하며, 시간이 지남에 따라 발전되어 안정화되는 공격자의 기술 수준을 예측하고 이에 대응할 수 있는 방어 전략을 수립할 수 있도록 한다.

V. 결 론

본 논문에서는 기존 CVSS의 한계점과 기존의 공격자의 기술 수준을 고려한 취약점 평가 관련 연구의 한계점을 도출하였다.

이를 위해 기존의 취약점 정보 외에 산업제어시스템 취약점 및 APT 공격 정보를 추가적으로 수집하였으며, 공격자의 기술 수준을 판단하기 위한 평가 대상 속성을 선정하고, 분류 기준을 정의하였다. 이를 기존 CVSS 기본 지수 평가 산출식에 반영하여 취약점의 정적 특성만이 아닌 시간의 흐름에 따라 변화하는 동적 특성이 함께 고려된 심각도 평가 방안을 제안하였다.

또한 선정한 대상 속성을 기반으로 수행한 평가 결과가 실제 시간의 흐름에 따른 위험도와 심각성을 반영하는지와 운영 기술 및 산업제어시스템 환경에서의 취약점에 대하여 해당 평가 방안이 적용 가능한지의 2가지 측면에서 사례연구를 수행하였다. 평가 결과, 각 시간축에 해당하는 취약점 및 익스플로잇 정보에 따른 그 가용 수준의 증가로 위험성과 긴급성이 반영된 점수가 산출됨을 확인하였다. 또한 실제 운영 기술 및 산업제어시스템 환경을 대상으로 한 사이버 공격에 악용됨에도 불구하고, 여전히 보안 조치 대상 기준 점수인 7.0이하의 심각도 점수를 가지는 취약점이 평가 방안 적용 결과 7.0 이상의 점수로 증가됨을 확인하였다.

이를 통해 본 연구에서 제안한 평가 방안이 시간의 흐름에 따른 공격자의 무기화 수준 추적이 가능함과 운영 기술 및 산업제어시스템 운영 환경에 적용 가능하고, 실제 위험성을 반영하는 취약점 심각도 점수 산출이 가능함을 확인하였다.

따라서 본 연구에서 제안하는 취약점 평가 방안을 활용한다면 정보 기술 분야 뿐 아니라, 운영 기술 및 산업제어시스템 분야에서 시간의 흐름에 따라 변화하는 취약점의 무기화 수준을 고려한 보안 조치 전략을 효율적으로 도출해낼 수 있을 것이다.

References

[1] R. Sharma, R. Sibal, and S. Sabharwal, "Software vulnerability prioritization using vulnerability description," International Journal of System Assurance Engineering and Management, Vol. 12, pp. 58-64, Jul. 2021.

[2] Yang, Heedong, et al. "Better Not to Use Vulnerability's Reference for Exploitability Prediction," Applied Sciences, Vol. 10, No. 7, pp. 2555-2565, Apr. 2020.

[3] Kim Kyung-ho, Weekly Technology Trend, Industrial Control System Security, No. 1981., Institute for Information & communication Technology Planning & evaluation, pp. 2-14, Jan. 2021.

[4] FIRST, "CVSS Documentation", https://www.first.org/cvss/specification-document, Apr. 2023

[5] Michael Thow, "Cyber Security Technical Assessment Methodology (TAM): OT Assessment First Principles," EPRI Inc,

pp. 1-23, Dec. 2019.
[6] EPRI, “Cyber Security Technical Assessment Methodology: Risk Informed Exploit Squence Identification and Mitigation, Revision 1,” EPRI Inc, Nov. 2018.
[7] Jung, Bill, Yan Li, and Tamir Bechor. ″CAVP: A context-aware vulnerability prioritization model,″ Computers & Security, 116:102639, Feb. 2022.
[8] U.K. Singh, and C. Joshi, “Quantitative security risk evaluation using CVSS metrics by estimation of frequency and maturity of exploit,” In Proceedings of the World Congress on Engineering and Computer Science, Vol. 1, pp. 19-21, Oct. 2016.
[9] Bulut, Muhammed Fatih, et al. ″Vulnerability prioritization: An offensive security approach,″ arXiv preprint, arXiv:2206.11182, Jun. 2022.
[10] K.A. Farris, A. Shah, and G. Cybenko, R. Ganesan, S. Jajodia, “Vulcon: A system for vulnerability prioritization, mitigation, and management,” ACM Transactions on Privacy and Security (TOPS), Vol. 21, No. 16, pp. 1-28, Jun. 2018.
[11] NVD Data Feed for Vulnerabilities, “NVD CVE Data”, https://nvd.nist.gov/vuln/data-feeds, Apr. 2023
[12] Official Common Platform Enumeration (CPE) Dictionary, “CPE Dictionary”, ″https://nvd.nist.gov/products/cpe″, Apr. 2023.
[13] MITRE Common Weakness Enum eration, “Mitre CWE Data”, https:// cwe.mitre.org / data/downloads, Apr. 2023.
[14] MITRE Common Attack Pattern Enumeration and Classification, “Mitre CAPEC data”, https://capec. mitre.org/data/index.html, Apr. 2023.
[15] CISA ICS-CERT Advisories, “ICS-CERT A dviories”, https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A95, Apr. 2023.
[16] Exploit-DB, “Exploit”, https://exploit - db.com, Apr. 2023.
[17] Github, “PoC in Github”, https://github.com/nomi-sec/PoC-in-GitHub/, Apr. 202.
[18] CISA, “Known Exploited Vulner ability”, https://www.cisa.gov/known- exploited-vulnerabilities-catalog/, Apr. 2023.
[19] CISA, “National Cyber Awareness System”, https://www.cisa.gov/uscert /ncas/alerts/, Apr. 2023.
[20] Github, “Metasploit module data”, https://github.com/rapid7/metasploit-framework/tree/master/db, Apr. 2023
[21] MITRE, “CVE Numbering Authorities (CNAs)”, https://www.cve.org/Progra mOrganization/CNAs, Apr. 2023.

〈저자소개〉

윤 성 수 (Seong-Su Yoon) 학생회원
2021년 2월: 전남대학교 소프트웨어공학과 졸업
2023년 2월: 전남대학교 정보보안협동과정 석사 졸업
2023년 3월~현재: 전남대학교 정보보안협동과정 박사과정
〈관심분야〉 정보보호, 인공지능, 산업제어시스템 보안

엄 익 채 (Ieck-chae Euom) 종신회원
2003년 8월: 전남대학교 컴퓨터정보학부 학사 졸업
2015년 2월: 한국과학기술원 소프트웨어대학원 석사 졸업
2019년 2월: 전남대학교 정보보안협동과정 박사 졸업
2003년~2007년: LG이노텍, 주임연구원
2007년~2019년: 한전KDN, 차장
2019년 10월~현재: 전남대학교 시스템보안연구센터 소장, 데이터사이언스대학원 교수
〈관심분야〉 제어시스템보안, 스마트그리드 보안, 원자력 보안, 취약점 분석, 차세대인프라 보안, 스마트시티·공장 보안, AI기반 이상징후 탐지, 지능형 보안