소프트웨어 보안 취약점 평가 체계 동향

장대일 _ 한국인터넷진흥원 책임연구원

1. 머리말

어느 분야에서든 약점에 대한 위험(risk)을 평가하는 것은 취약점을 찾는 것만큼이나 중요하다. 위험은 일반적으로 위협 모델링(threat modeling)이나 코드 리뷰(code review), 침투 시험(penetration testing) 등의 방법을 통해 식별하는 것이 가능하고, 위험을 평가하기 위해 CVSS(Common Vulnerability Scoring System), CWSS(Common Weakness Scoring System)와 CWE/SANS Top 25 Most Dangerous Software Errors, The OWASP Risk Rating Methodology, DREAD model 등 다양한 보안취약점 평가 방법이 존재한다. 이를 위해 소프트웨어의 보안취약점은 미국 국립표준기술연구소(NIST)를 비롯하여 소프트웨어 보안취약점을 다루는 각 벤더별로 그 취약점을 평가하기 위한 체계를 갖추고 있다. 이중 NIST의 지원을 받는 MITRE에서 관리하는 CVSS가 보안취약점 평가를 위한 표준으로 사용되고 있다.

CVSS는 MITRE에서 관리하는 보안 취약점 관리 체계인 CVE(Common Vulnerabilities and Exposure)의 요소 중 하나로, 보안취약점이 동작하는 환경, 절차 및 파급력 등을 통해 취약점을 진단하고 평가할 수 있는 기준이다. 2005년 2월에 최초로 발표된 CVSS는 국립 취약점 DB(NVD, National Vulnerability Database)에서 볼 수 있으며, 2007년에 발표된 CVSS v2.0과 2015년 6월에 발표된 CVSS v3.0, 그리고 2019년 6월에 CVSS v3.1이 발표되었다. 본고에서는 CVSS v2.0과 CVSS v3.0 및 CVSS v3.1을 사용하여 취약점을 평가할 때 점수의 차이를 검토할 것이다.

2. CVSS 동향

2.1 CVSS v2.0에서 CVSS v3.0 변경 사항

CVSS v2.0 기본 점수 범위에 대해 '낮음', '중간' 및 '높음'의 정성적 심각도 순위를 제공했지만, CVSS v3.0은 응용프로그램에 속하는 보다 정확한 취약점을 반영하기 위해 '위험' 순위를 포함하는 여러 가지 변경 사항을 도입했다.

기본 점수, 임시 점수 및 환경 점수의 세 가지 메트릭 그룹은 모두 동일하게 유지되었지만 범위(S)

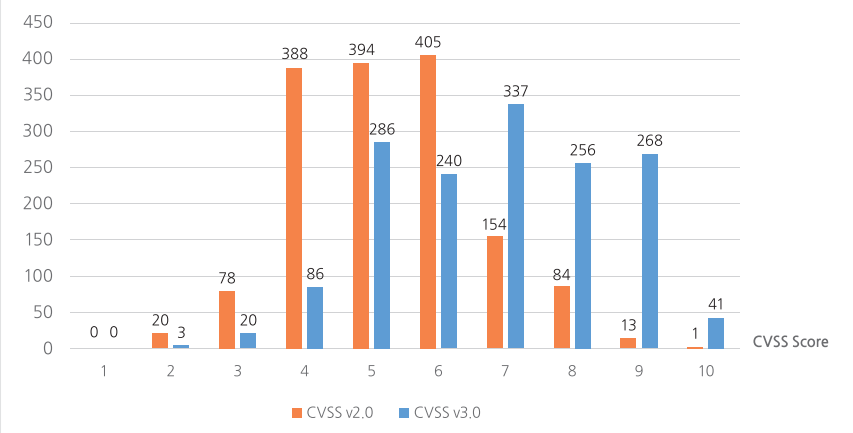
<표 1> CVSS 점수 범위에 따른 심각도 변화

CVSS v2.0		CVSS v3.0	
심각도(Severity)	기본점수 범위	심각도(Severity)	기본점수 범위
낮음(Low)	0.0-3.9	낮음(Low)	0.1-3.9
중간(Medium)	4.0-6.9	중간(Medium)	4.0-6.9
높음(High)	7.0-10.0	높음(High)	7.0-8.9
		위험(Critical)	9.0-10.0

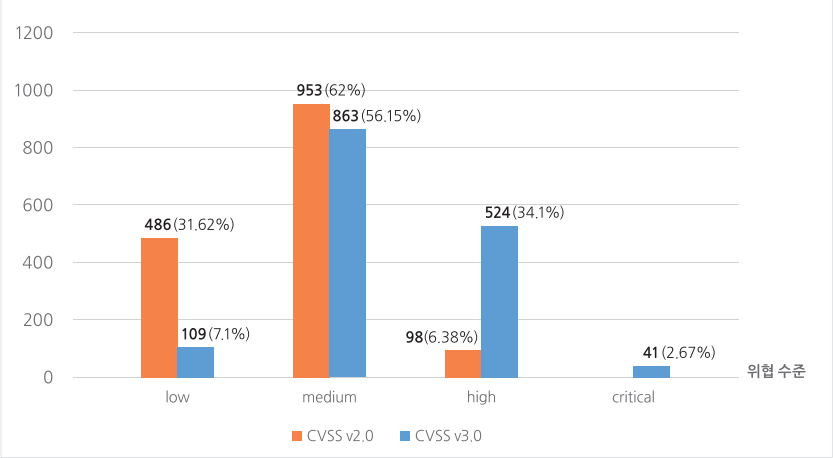
<표 2> CVSS 메트릭 변화

구분		CVSS v2.0	CVSS v3.0
기본 점수	Exploitability Metrics	Attack Vector(AV)*	Attack Vector(AV)*
		Access Complexity(AC)*	Attack Complexity(AC)*
		-	User Interaction(UI)*
		Authentication(Au)*	Privileges Required(PR)*
	Impact Metrics	Confidentiality Impact(C)*	Confidentiality Impact(C)*
		Integrity Impact(I)*	Integrity Impact(I)*
		Availability Impact(A)*	Availability Impact(A)*
		-	Scope(S)*
임시 점수		Exploitability(E)	Exploitability(E)
		Remediation Level(RL)	Remediation Level(RL)
		Report Confidence(RC)	Report Confidence(RC)
환경 점수	General Modifiers	Collateral Damage Potential(CDP)	-
		Target Distribution(TD)	-
	Impact Subscore Modifiers	Confidentiality Requirement(CR)	Confidentiality Requirement(CR)
		Integrity Requirement(IR)	Integrity Requirement(IR)
		Availability Requirement(AR)	Availability Requirement(AR)
	Modified Base Metrics		Modified Attack Vector(MAV)
			Modified Attack Complexity(MAC)
			Modified User Interaction(MUI)
			Modified Privileges Required(MPR)
			Modified Confidentiality Impact(MC)
			Modified Integrity Impact(MI)
			Modified Availability Impact(MA)
			Modified Scope(MS)

및 사용자 상호 작용(UI)과 같은 새로운 메트릭이 추가되었다. 또한 인증(Au)과 같은 이전 메트릭은



[그림 1] 동일 취약점 대상 CVSS 버전별 점수 차이



[그림 2] 동일 취약점 대상 CVSS 버전별 위협수준 차이

PR(Privileges Required)과 같은 최신 메트릭으로 변경되었다. 범위 메트릭은 동일한 권한으로 관리되는 리소스에만 영향을 줄 수 있는 악용된 취약점을 구별한다. 이 경우 취약한 구성 요소와 영향을 받는 구성 요소는 동일하다. 환경 메트릭(Environmental Metrics) 그룹은 수정된 기본 메트릭(Modified Base Metrics)을 새로 추가하여 분석가가 조직에 영향을 미치는 호스트를 기준으로 CVSS 점수를 사용자 정의하여 필요할 때 상황에 맞게 만들 수 있도록 수정했다.

2.1.1 CVSS v3.0 적용 결과

2016년 발표된 CVE 취약점 대상 CVSS v2.0과 CVSS v3.0을 통해 취약점을 평가한 결과에 대한 점수분포는 [그림 1]과 같다. 현재 CVE 리스트 중 CVSS v3.0이 포함된 1,537개 취약점을 대상으로 진행하였다.

동일한 취약점군을 대상으로 CVSS v2.0 평균 4.97, CVSS v3.0 평균 6.30으로 CVSS v3.0이 CVSS v2.0에 비해 취약점의 전체 기본점수가 높게 표현되는 것을 확인할 수 있다. 해당 취약점 중 CVSS v3.0의 점

수가 CVSS v2.0 점수와 비교해서 낮아진 경우는 총 215개 케이스이고, 평균 0.59가 낮아졌다. 하지만 취약점 중 CVSS v3.0의 점수가 CVSS v2.0 점수와 비교해서 높아진 경우 평균 1.69가 높아졌다. 각 산정된 점수를 위협 수준으로 분류할 경우 [그림 2]와 같다. 낮은 위협수준을 갖는 취약점은 24.52%, 중간 위

<표 3> CVSS v3.1 변경 사항

대상			추가 및 변경 사항
Base Matrics	Attack Vector(AV)	Adjacent(A)	· 논리적으로 인접하거나 신뢰할 수 있는 네트워크 (MPLS, VPN 등)에 대한 공격 벡터를 포함 · 리소스가 방화벽 뒤에 있는 경우 수정된 공격 벡터 환경 지표 사용에 대한 새로운 지침이 포함
		Local(L)	· 네트워크 바운드의 범위 변경(로컬 취약점을 발현시키기 위한 접근 방법이 내부 접근, 혹은 원격 접근 모두 허용) · 사회공학적인 방법을 통한 사용자 간 상호작용에 의존하여 취약점을 악용하는 기법 포함
	Scope	Changed(C)	· 한 보안 기관이 관리하는 구성 요소의 취약점이 다른 보안 기관이 관리하는 리소스에 영향을 줄 수 있으면 범위가 변경
Environmental Score	Security Requirements	Confidentiality Requirement(CR)	· 최상위로 분류된 데이터를 저장하는 장치는 높음(High)으로 평가 · 비공개 데이터지만 최상위 레벨이 아닌 데이터를 저장하는 장치는 중간(Medium)으로 평가 · 공개적으로 공유할 수 있는 데이터를 저장하는 장치는 낮음(Low)으로 평가 · 네트워크 장비는 일반적으로 중간으로 평가 · 암호화 없이 로그인 정보를 저장하는 장치는 높음으로 평가
		Integrity Requirement(IR)	· 금전적 거래 데이터 또는 개인 식별 정보(PII)가 포함된 장치는 높음으로 평가 · 비즈니스 또는 위험 관리 결정을 내리는 데 직접 사용되는 데이터가 포함된 장치는 최소 중간 등급 · 건강 결정을 내리는 데 직접 사용되는 데이터가 포함된 장치는 높음으로 평가 · 네트워크 장비는 일반적으로 중간으로 평가 · 방화벽은 룰셋 등 민감정보로 인해 높음으로 평가
		Availability Requirement(AR)	· 24시간 미만의 복구 요구 사항으로 등급이 매겨진 장치는 높음으로 평가 · 1~5일 사이의 복구 요구 사항으로 등급이 매겨진 장치는 중간으로 평가 · 복구 요구 사항이 5일 이상인 장치는 낮음으로 평가 · 클러스터 된 장비나 전체 용량에 대한 중복성이 보장(full capacity redundancy)되는 장비는 낮음으로 평가 · 트랜잭션 목적으로 빠른 응답 시간을 가져야 하는 장치는 높음으로 평가
	Modified Impact Sub Score	Modified Scope Changed	산식: 7.52 × (MISS-0.029) - 3.25 × (MISS-0.02)[15] → 수정 산식: 7.52 × (MISS - 0.029) - 3.25 × (MISS × 0.9731 - 0.02)[13]
반올림 함수(RoundUp)			· 작은 부동 소수점 부정확성으로 인해 다른 점수를 생성할 가능성을 최소화하기 위해 보다 정확하게 정의됨

			function Roundup (input):
			int_input = round_to_nearest_integer (input * 100000)
			if (int_input % 10000) == 0:
			return int_input / 100000.0
			else:
			return (floor(int_input / 10000) + 1) / 10.0

취약점 체인			· 단일 공격 과정에서 여러 취약점이 악용되어 호스트 또는 응용 프로그램을 손상시키는 상황을 수용 · 공식적인 지표는 아니지만 이러한 종류의 공격을 평가할 때 분석가를 위한 지침으로 포함

협수준을 갖는 취약점은 5.85% 낮아진 반면, 높은 위협수준을 갖는 취약점은 27.72%, 위험한 위협수준을 갖는 취약점은 2.67% 증가하였다.

2.2 CVSS v3.0에서 CVSS v3.1 변경사항

CVSS v3.0에서 v3.1로 변경은 새로운 메트릭이나 메트릭 값을 도입하거나 기존 공식을 크게 변경하지 않은 상태로 표준을 좀 더 명확하게 하고 개선하는 데 중점을 두었다. CVSS가 위험 평가의 절대적인 요소가 되고 있는 문제를 해결하기 위해 다양한 요소를 고려한다. 상세 변경 사항은 〈표 3〉과 같다.

CVSS v3.0에서 CVSS v3.1로의 변화는 기존 v2.0에서 v3.0으로 변화만큼 크지 않지만 기존에 가지고 있던 오류를 상당 부분 해결한 것으로 볼 수 있다. 예를 들어 반올림 함수를 수정함으로써 CVSS v3.1에서 약 7% 수준의 메트릭 조합이 v3.0보다 0.1 높아졌고, 약 1% 수준의 메트릭 조합이 v3.0보다 0.1 낮아졌다.

3. 맺음말

보안취약점을 평가하고 위험 등급을 통한 취약점 관리를 위해 다양한 기준들이 제시되고 있다. 그 중 CVSS는 MITRE에서 관리하는 국제 표준으로 보안취약점을 평가하기 위해 가장 많이 사용되고 있다. 이에 본고에서는 CVSS v2.0부터 v3.1까지 변화를 확인하였다. 위에서 살펴본 바와 같이, 고도화되는 보안취약점에 대응하기 위해 기존에 가지고 있던 오류를 해결하고 보완하며 보안취약점 평가 체계 또한 진화하고 있다. 다만 국내 보안생태계에 맞는 보안취약점 평가 체계가 필요할 것으로 판단된다.

※ 본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행됨[No. 2017-0-00184, 자기학습형 사이버 면역 기술 개발].

[참고문헌]

[1] Common Vulnerability Scoring System version 3.1: User Guide
[2] Common Vulnerability Scoring System version 3.0: User Guide
[3] Common Vulnerability Scoring System version 2.0: User Guide
[4] Common Vulnerability Scoring System version 3.1: Specification Document
[5] Common Vulnerability Scoring System version 2.0: Specification Document

[주요 용어 풀이]

- CVE(Common Vulnerabilities & Exposures): 공통 보안 취약성 및 노출, 보안 취약성과 기타 정보 보안 노출 사항을 기록한 규격화된 목록. 보안 도구 제조업체, 대학 연구소, 정부 기관, 기타 보안 전문가 등 수많은 보안 관련 기관의 대표들이 포함된 CVE 편찬위원회에서 만드는 것으로 보안 취약성 데이터베이스와 보안 도구를 통한 데이터 공유를 용이하게 하기 위한 것이다. 이 목록은 CVE 명칭(일련번호 포함), 취약성 및 노출 개요, 대응 참조 사항 등으로 작성된다.
- 침투 시험(penetration test): 시스템의 보안 취약점을 찾거나 또는 접근 권한을 얻기 위해 시도하는 공격. 침투 시험은 정보 시스템의 취약점이 있는지 또는, 취약점이 실제로 악용될 수 있는지를 확인하기 위해 평가자가 직접 침투를 실시하는 모의 해킹(hacking simulation)에 사용된다.