KIPS Trans. Comp. and Comm. Sys.
Vol.8, No.7 pp.177~180 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2019.8.7.177

A Study on Layered Weight Based Vulnerability Impact Assessment Scoring System

Youngjong Kim†

ABSTRACT

A typical vulnerability scoring system is Common Vulnerability Scoring System(CVSS). However, since CVSS does not differentiate among the individual vulnerability impact of the asset and give higher priority for the more important assets, it is impossible to respond effectively and quickly to high-risk vulnerabilities on large systems. We propose a Layered weight based Vulnerability impact assessment Scoring System which can hierarchically group the importance of assets and weight the number of layers and the number of assets to effectively manage the impact of vulnerabilities on a per asset basis.

Keywords : CVE, CVSS, Vulnerability Impact Assessment Scoring System

계층적 가중 기반의 취약점 영향성 평가 스코어링 시스템에 대한 연구

김 영 종†

요 약

대표적인 취약점 스코어링 시스템은 CVSS다. 하지만 CVSS는 취약점이 자산에 미치는 영향성 관점을 평가 하지 않아 사용되지 않거나 중요도가 낮은 자산에 대해서도 동일한 우선순위로 처리해야하기 때문에 대규모 시스템의 위험도가 높은 취약점의 경우 효과적이고 신속한 대응을 할 수 없다. 시스템 구성을 계층화 하고, 계층 간의 그리고 계층내의 중요도에 따른 가중을 평가하는 영향성 관점의 평가 시스템인 계층적 가중 기반의 취약점 영향성 평가 스코어링 시스템을 제안한다.

키워드 : 보안, 취약점, 취약점 영향성 평가

1. 서 론

기술의 발전에 따른 인터넷 보급과 모바일기기의 확산 등에 따라 정보 시스템에 대한 이용과 사고가 동시에 기하급수적으로 증가하며 정보 시스템에 대한 의존도가 높아지는 추세가 지속되고 있어 정보시스템의 위협관리(IT Risk Management)는 매우 중요하다[1]. 정보시스템의 보안을 위협하는 보안 취약점 식별 시, 해당 취약점이 전체 시스템에 미치는 영향성 평가를 통한 정보시스템 위협 관리는 매우 중요하다.

정보보호담당자의 정보보호 능력 및 수준에 따라 체계 정보보호대책 수준이 상이하기 때문에, 보안 취약점 식별 시, 전체 시스템을 구성하는 구성시스템과 운영시스템, 운영망등의 각 운영 자산의 중요도에 기반한 영향성 평가에 따라 대응의 우선순위를 가지며 전체 시스템 차원에서 보안 위협을 관리할 수 있어야 한다.

2. 관련 연구

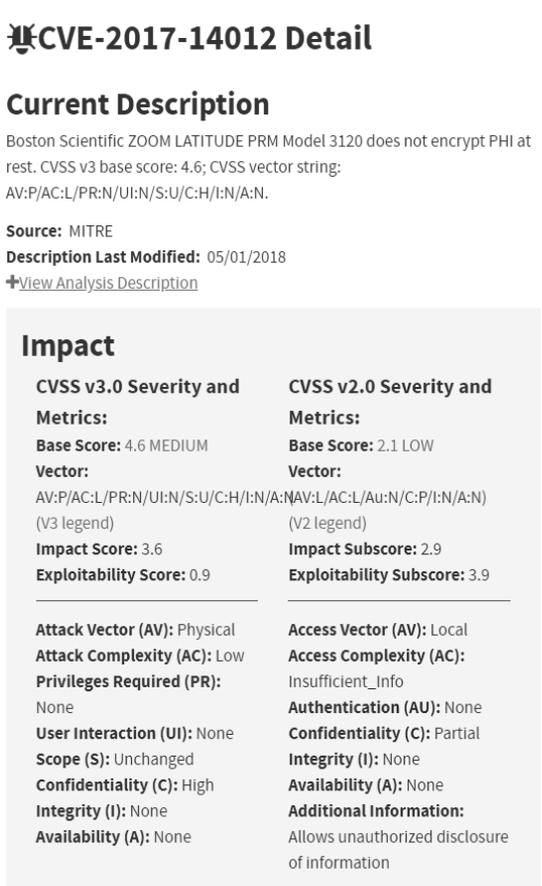
Common Vulnerabilities and Exposure(CVE)[2]는 1999년 1월 미국 퍼듀 대학에서 개최된 "2nd Workshop on Research with Security Vulnerability Databases"에서 비영리 법인인 MITRE의 제안에 의해서 구축 되었으며, 취약점 식별 도구 및 취약성 대책 정보 제공 서비스에 사용한다.

CVE는 1999년 이후 약 11만 2천개 이상의 취약점 정보를 구축하였고 최근에는 더 빠른 속도로 구축된 취약점 정보가 증가하고 있으며 CVE는 본래 취약점 정보 데이터베이스가 아닌 만큼, 간단한 요약과 관련 정보 정도만 제공한다.

CVE는 'CVE-1999-0067', 'CVE-2014-10001', 'CVE-2014-

† 종신회원 : 숭실대학교 소프트웨어학부 교수
Manuscript Received : January 24, 2019
Accepted : March 13, 2019
* Corresponding Author : Youngjong Kim(youngjong@ssu.ac.kr)

100001'과 같이 "CVE-XXXX-XXXX"와 같은 형태의 고유의 식별 번호를 부여한다. Fig. 1은 CVE-2017-14012의 검색 결과[3]이다.



CVE-2017-14012 Detail

Current Description

Boston Scientific ZOOM LATITUDE PRM Model 3120 does not encrypt PHI at rest. CVSS v3 base score: 4.6; CVSS vector string: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

Source: MITRE
Description Last Modified: 05/01/2018
View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:	CVSS v2.0 Severity and Metrics:
Base Score: 4.6 MEDIUM	**Base Score:** 2.1 LOW
Vector: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (V3 legend)	**Vector:** (AV:L/AC:L/Au:N/C:P/I:N/A:N) (V2 legend)
Impact Score: 3.6	**Impact Subscore:** 2.9
Exploitability Score: 0.9	**Exploitability Subscore:** 3.9
Attack Vector (AV): Physical	**Access Vector (AV):** Local
Attack Complexity (AC): Low	**Access Complexity (AC):** Insufficient_Info
Privileges Required (PR): None	**Authentication (AU):** None
User Interaction (UI): None	**Confidentiality (C):** Partial
Scope (S): Unchanged	**Integrity (I):** None
Confidentiality (C): High	**Availability (A):** None
Integrity (I): None	**Additional Information:** Allows unauthorized disclosure of information
Availability (A): None	

Fig. 1. CVE-2017-14012, Data from National Institute of Standards and Technology, U.S. Department of Commerce[3]

Common Vulnerability Scoring System(CVSS)[4]는 수많은 이 기종의 하드웨어와 소프트웨어에 걸쳐 다양하게 발생하는 취약점의 등급을 평가할 때 사용한다.

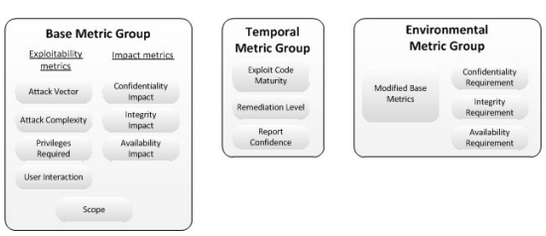


Fig. 2. CVSS v3.0 Metric Groups, Data from FIRST.Org, Inc.[4]

CVSS의 매트릭 그룹은 Fig. 2와 같이 3가지 매트릭 그룹을 가지고 있다. CVE에 대한 CVSS 점수는 CVSS의 3가지 매트릭 그룹인 기본 메트릭 그룹(Base Metric Group), 임시 메트릭 그룹(Temporal Metric Group), 환경 메트릭 그룹(Environmental Metric Group)의 3~6개의 구성되어 있으며, CVSS의 환경 메트릭 그룹은 자산에 대해 전체 시스템 관점의 영향성 관점의 평가를 하지 않는다.

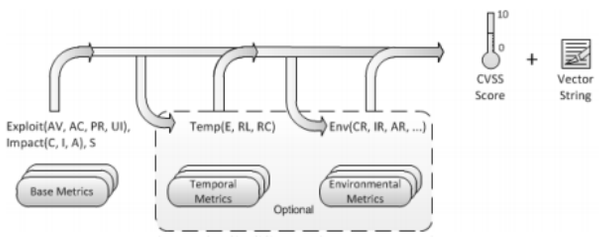


Fig. 3. CVSS Metrics and Equations, Data from FIRST.Org, Inc.[4]

CVSS는 Fig. 3과 같은 방식으로 계산되어 0.0에서 10.0 사이의 값으로 위험도 점수를 평가한다.

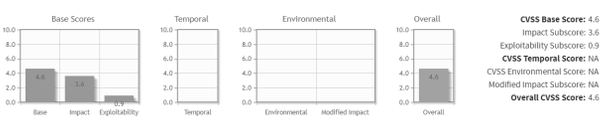


Fig. 4. The Components of the CVSS Score for CVE-2017-14012 Data from FIRST.Org, Inc.[5]

CVSS는 CVE-2017-14012에 대해 Fig. 2의 Metric Groups에 대해 Fig. 3과 같은 방식으로 Fig. 4와 같이 계산되어 취약점 정보 DB인 NVD[6]를 통해 등급이 평가되어 점수화 된다.

3. 계층적 가중 기반의 취약점 영향성 평가 스코어링 시스템

본 논문에서는 시스템 구성을 분석하여 계층(Layer)을 나누고, 계층 간의 그리고 계층내의 중요도에 따른 가중을 통해, 획일화된 평면적 취약점 평가 체계에서는 판단하지 않는, 계층과 계층내의 중요도 변수에 따른 자산의 중요도 기반의 영향성 평가를 할 수 있도록, 계층적 가중기반의 취약점 영향성 평가 스코어링 시스템(Layered weight based Vulnerability impact assessment Scoring System, LVSS)을 제안한다. 제안된 LVSS는 Equation (1)과 같다.

$$\text{자산평가 점수} = \left(\frac{10 * N_1}{S_1} + \left\{ \frac{\sum_{i=1}^{N_2} W * X_i}{2 * N_2} * 10 - \alpha + \frac{\alpha * N_2}{S_2} \right\} \cdots \frac{10 * N_L}{S_L} \right) / L \quad (1)$$

주: S_1 = 자산계층 1의 총 수, S_2 = 자산계층 2의 총 수, S_L = 자산계층 L의 총 수, N_1 = 영향을 받는 자산계층 1의 수, N_2 = 영향을 받는 자산계층 2의 수, N_L = 영향을 받는 자산계층 L의 수, W = 자산계층 2 내의 가중치: 2(High)/1.5(Medium)/1(Low), Xi = 자산계층 2내의 자산분류, α = 보정계수, L = 자산계층 수

L은 분석된 시스템 구성상 단계를 의미하는 계층수이며, 계층을 계층내의 자산의 개수만으로 영향성 평가를 계산할 경우에는 계산식 $\frac{10*N_1}{S_1}$ 를 사용하고 , 계층내의 자산분류별 중요도에 따라 영향성 평가를 계산할 경우에는 계산식 $\frac{\sum_{i=1}^{N_2} W*X_i}{2*N_2}*10-\alpha+\frac{\alpha*N_2}{S_2}$ 을 사용하여 계층내의 자산분류별 중요도에 따라, 가중치를 추가하고 보정계수로 해당 계층의 값을 자산의 개수만으로 영향성을 평가한 계산식과 같은 범위로 보정한다. X_i 는 계산식 내의 자산분류를 의미한다.

4. 적 용

4.1 적용 환경

Table 1과 같이 일반적인 구성인 구성시스템(System)과 운영시스템(Service), 운영망(Network)으로 구성된 3단계의 계층으로 설정하였다.

Table 1. Detail Information of Layer for Classification

Layer	Classification	Detail
1	System	App Server, Gateway Server, DB Server and more
2	Service	ERP, Web Service and more
3	Network	Internal Network, External Network, Region Network and more

Table 2와 같이 3 계층을 가지며, 구성시스템의 총수는 5개이며, 운영시스템은 12개이고 운영망의 총수는 4개인 시스템으로 설정하였다.

Table 2. Environments for Simulation Experiments

Classification	No. of Assets
Total No. of Layers	3
Total No. of Systems	5
Total No. of Services	12
Total No. of Networks	4

점수체계는 0~10까지로 구분하였으며 이를 위해 보정계수 4를 주어 가정한 LVSS 계산식은 Equation (2)와 같다.

$$\text{자산평가점수} = \left(\frac{10*C}{5}+\left\{\frac{\sum_{i=1}^{M} W*X_i}{2*M}*10-4+\frac{4*M}{12}\right\}+\frac{10*O}{4}\right)/3 \quad (2)$$

주: C = 영향 받는 구성시스템 수, M = 영향 받는 운영시스템의 수, O = 영향 받는 운영망의 총 수

Equation (2)의 $\frac{10*C}{5}$ 는 1계층으로, 취약점이 영향을 미치는 구성시스템의 개수 대한 가중치를 계산하고, Equation (2)의 $\frac{\sum_{i=1}^{M} W*X_i}{2*M}*10-4+\frac{4*M}{12}$ 는 2계층으로 운영시스템간의 가중치를 2(High)/1.5(Medium)/1(Low)로 하여, 취약점이 영향을 미치는 운영시스템 각각의 가중치를 계산하며, Equation (2)의 $\frac{10*O}{4}$ 는 3계층으로 취약점이 영향을 미치는 운영망의 개수 대한 가중치를 계산한다. LVSS 로 계산된 값을 점수화 하여 CVE 점수와의 차이점에 대해 분석하였다.

4.2 CVE-2017-14012 에 대해 구성시스템의 개 수와 운영망의 개수에 차등을 준 결과 분석

Table 2의 실험 시스템에 대해, Table 3과 같이 취약점에 영향을 받는 운영시스템의 수는 10개로 동일하게 하고, 영향받는 구성시스템과 운영망의 개수를 달리하여 가중을 설정하여 구성된 예시(Case)에 대해 LVSS로 계산하여 CVSS 점수와 비교해 보았다.

Table 3. Detail Information of Simulation Cases for No. of Affected Assets on Classification of Sitting Postures

Case	No. of Systems	No. of Services	No. of Networks
1	1	High 10	1
2	1	High 2, Low 8	1
3	3	High 10	2
4	5	High 10	4

Equation (2)의 스코어링 방식에 따라, 예시 1을 계산하면 Equation (3)과 같다.

$$\approx 4.61 = \left(\frac{10*1}{5}+\left\{\frac{2*10}{2*10}*10-4+\frac{4*10}{12}\right\}+\frac{10*1}{4}\right)/3 \quad (3)$$

Equation (2)의 스코어링 방식에 따라, 예시 2를 계산하면 Equation (4)와 같다.

$$\approx 3.27 = \left(\frac{10*1}{5}+\left\{\frac{(2*2)+(1*8)}{2*10}*10-4+\frac{4*10}{12}\right\}+\frac{10*1}{4}\right)/3 \quad (4)$$

Equation (2)의 스코어링 방식에 따라, 예시 3을 계산하면 Equation (5)과 같다.

$$\approx 6.77 = \left(\frac{10*3}{5}+\left\{\frac{2*10}{2*10}*10-4+\frac{4*10}{12}\right\}+\frac{10*2}{4}\right)/3 \quad (5)$$

Equation (2)의 스코어링 방식에 따라, 예시 4를 계산하면 Equation (6)과 같다.

$$\approx 9.78 = \left(\frac{10*5}{5}+\left\{\frac{2*10}{2*10}*10-4+\frac{4*10}{12}\right\}+\frac{10*4}{4}\right)/3 \quad (6)$$

4.3 결과분석

CVE-2017-14012의 CVSS점수는 4.6이다. CVE-2017-14012에 대해, 예시 1, 2, 3, 4를 LVSS로 계산한 결과를 정리한 것과 CVSS값을 비교하면 Table 4와 같다.

Table 4. Comparison the Scores of CVSS and LVSS in Case 1, 2, 3, 4

Case	CVSS Score	LVSS Score
1	4.6	4.6
2	4.6	3.3
3	4.6	6.8
4	4.6	9.8

Table 4의 예시 1은 Table 3의 예시1과 같이 영향을 받는 구성시스템과 운영망이 하나고 영향을 받는 운영시스템이 High 10개인, CVSS 점수와 동일한 영향을 받는 예시로 Table 4의 예시1과 같이 LVSS는 CVSS의 점수는 같다.

Table 3의 예시 2와 같이 취약점에 대해 영향을 받는 운영시스템의 중요도가 Table 3의 예시 1 보다 낮은 8개가 Low 시스템인 경우 영향성을 반영한 LVSS 점수는 Table 4의 예시 2와 같이 CVSS보다 낮게 나오는 것을 확인할 수 있다.

Table 3의 예시 3과 같이 운영시스템의 영향성은 같고, 영향을 받는 구성시스템과 운영망이 3개와 2개로 늘어날 경우, Table 4의 예시 3과 같이 CVSS 점수보다 높게 나오는 것을 확인할 수 있다.

Table 3의 예시 4와 같이 운영시스템의 영향성은 같고, 영향을 받는 구성시스템과 운영망이 5개와 4개로 더 늘어날 경우 Table 4의 예시 4와 같이 CVSS 점수보다 매우 높게 나오는 것을 확인할 수 있다.

Table 4의 비교 결과와 같이 영향성 평가가 반영된 LVSS는 영향 받는 구성시스템의 개수와 운영망의 개수가 다르며, 운영시스템의 중요도가 다를 경우, 영향 받는 수와 중요도에 따른 영향성 평가에 따라 점수가 낮거나 높게 나옴을 확인할 수 있다.

5. 결 론

전체시스템의 구성에 따른 취약점에 대해 영향을 받는 자산계층과 분류의 중요도에 따라 보안 취약점이 가지는 영향성 평가는 매우 중요하다. CVSS 점수를 기반으로 취역점 자체의 중요도를 평가하고, 제안된 LVSS 점수를 통해 영향성 평가를 수행하면 취약점에 대해 전체 시스템관점의 영향성 평가가 가능하며, 우선순위에 기반한 효과적이고 신속한 대응이 가능하다. 제안된 계층적 가중 기반의 취약점 영향성 평가 스코어링 시스템을 통해 효과적인 영향성 평가를 할 수 있음을 확인하였다.

향후 연구 방향으로는 좀 더 다양한 시스템 환경에서 제안된 방식을 확대 적용할 수 있도록, 세분화된 연구를 수행하는 것이다.

References

[1] Enterprise Risk Management - Integrated Framework - COSO [Internet], https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf.

[2] Common Vulnerabilities and Exposure(CVE) [Internet], https://cve.mitre.org/about/index.html.

[3] CVE-2017-14012 Detail [Internet], https://nvd.nist.gov/vuln/detail/CVE-2017-14012.

[4] Common Vulnerability Scoring System v3.0: Specification Document [Internet], https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf.

[5] Common Vulnerability Scoring System Calculator [Internet], https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2017-14012&vector=AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

[6] NATIONAL VULNERABILITY DATABASE [Internet], https://nvd.nist.gov/.

김 영 종

https://orcid.org/0000-0003-0811-0215

e-mail : youngjong@ssu.ac.kr

1996년 한글과컴퓨터 연구원

2005년 시큐어소프트 기술이사

2006년 하우리 대표이사

2007년 오픈소스커뮤니티연구소 소장 및 열린사이버대학교 정보지원처장

2019년~현 재 숭실대학교 소프트웨어학부 부교수

관심분야 : Security, Blockchain & Cloud Computing