Ivsev: Improved Vulnerability Scoring Mechanism With Environment Representative And Vulnerability Type

Gagandeep Chawla, Dr. Neeraj Sharma, Dr. Narender Kumar Rawal

Abstract- A failure to make security a priority while developing software invites intruders to perform malicious activities like money laundering, social engineering attack and loss of other important business information. Computer systems such as Servers, Workstations and even mobiles are vulnerable to attack from many avenues. A single severe vulnerability that allows intruders to get root access to the system is probably more crucial than several low severe vulnerabilities. A successful recognition of vulnerability plays an important role in lowering down the risk of attacks. For years, researchers and other institutions are working for the betterment of vulnerability scoring systems. Numerous security measures and tools are available which makes the software much harder for intruders. Meanwhile security breaches and risk is also rising, which doesn't stop with the development of security techniques. Once vulnerability is detected, it is important to release a patch at the earliest before it makes any damage. Scoring systems like CVSS is used to produce numerical score of vulnerability reflecting its severity level. On the basis of evaluated score security team could assess the security situation of the system including host and network. CVSS uses three metric groups (Base, Temporal and Environmental) to calculate the severity of vulnerabilities. In this paper, we propose a mechanism IVSEV (Improved Vulnerability scoring system with 'Environment representative' and 'Vulnerability type') for the better assessment of vulnerabilities. The proposed IVSEV adds two new features ER "Environment Representative" & VT "Vulnerability type" into conventional CVSS-v2 base score equation.

Index Terms: CVSS, IVSE, IVSV, NVD, IVSEV, Base score, Vulnerability.

1. INTRODUCTION

Vulnerability detection is a critical issue in the community of Software security. Any tiny vulnerability or a small security mistake can cause a whole system to crash [1]. Due to raised complexity of software, it is difficult to completely avoid the vulnerabilities. Excessive use of automated equipment and hardware almost in every area is inviting companies to develop software to operate them [2]. The continuous dependency on software brings associated risks; cyber-attacks, threats and vulnerabilities. Hence, it is of high importance to identify these risks early in the requirement phase [3],[4]. CVSS (Common Vulnerability Scoring System) is a universal de facto standard that plays a significant role in lowering down the risk of vulnerabilities [5]. Basically, CVSS-v2 has three metric groups (Base, Temporal and Environmental). Base group is mandatory to use whereas the other two i.e. "temporal metrics" and "Environmental metrics" are optional to use. The first group of CVSS i.e. Base group consists of the characteristics of the vulnerabilities. These characteristics do not change or modify over time. The second group i.e. The temporal group also consist of characteristics but these changes over time. And finally the environmental group includes the characteristics that are exclusive to each user's environment. The score calculated by CVSS is numerical that ranges from 0.0 to 10.0. Where score 0.0 signifies the least severe value and score of 10.0 signifies the most severe value.

After extensive literature survey and detailed study we noticed that none of the analyst used 'Environment representative' and 'Vulnerability type' for base score improvement. As per our study we found that these factors are very important to implement in CVSS-v2 base score equation as vulnerabilities have different impact on different operating environments. Ayodelel Oluwaseun Ibidapo, Pavol Zavarsky in their paper [6] suggested to use 'environmental metrics' to get true value of vulnerability. Georgios Spanos, Angeliki Sioziou in their paper [7] suggested to include a new factor 'Vulnerability type' to enhance the scoring mechanism.In this paper, we have proposed a new modified base score formula IVSEV (Improved Vulnerability scoring system with Environment representative and Vulnerability type). Environment representative contains three metric values i.e. Linux/Windows/Mac. Vulnerability type factor contains four most common types of vulnerabilities namely authentication weakness, buffer overflow, unvalidated input and race condition. Results obtained from IVSEV shows that the new scoring technique do impact on prioritizing vulnerabilities and helps security managers to release their patches. IVSEV takes 'environment representative' factor from our proposed model IVSE [8] and takes 'vulnerability type' factor from our proposed model IVSV [9]. Section 2 contains the brief description of the proposed IVSE and IVSV.

2. Brief Description of the Proposed IVSE and IVSV

2.1 Proposed IVSE (Improved Vulnerability Scoring System with Environment Representative)

Over the past several years, many security organizations and IT vendors are trying to improve the vulnerability scoring systems. Due to the continuous growth of vulnerabilities and bugs along with increase in demand of software, the improvement in scoring mechanism is a never ending process. The proposed IVSE is a scoring mechanism developed for the better assessment of vulnerabilities in software. This mechanism is basically an improvement over original CVSS-v2 base score formula as it includes the 'environment representative' in the base score calculation. CVSS-v2 base metric considers six factors to calculate the base score as given in fig 1.

- *Gagandeep Chawla, Pursuing Ph.D. in Applied Science (Computer Applications) from Punjab Technical University, Jalandhar, India. E-mail: gagans_chd@yahoo.com*
- *Dr. Neeraj Sharma, Ph.D., MBA, MCA from Punjab University, Chandigarh. E-mail: nrjsharma@yahoo.com*
- *Dr. Narender Kumar, Computer Science and Engineering, H.N.B. Garhwal University, India E-mail: narenrawal@gmail.com*

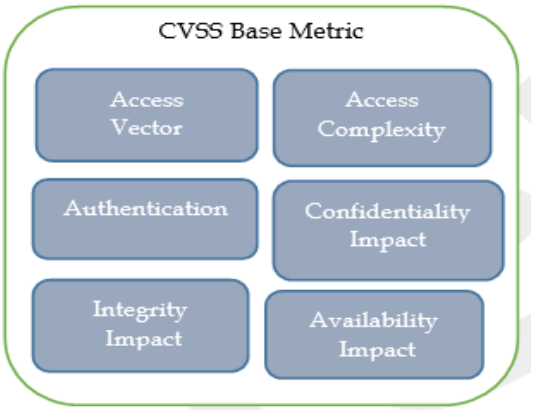


Fig.1. Base metric group of CVSS

After analyzing CVSS-v2 scoring mechanisms it has been observed that the 'Environment representative' should be included as an important part of CVSS-v2 base score formula. Fig 2 shows the proposed IVSE metric group.

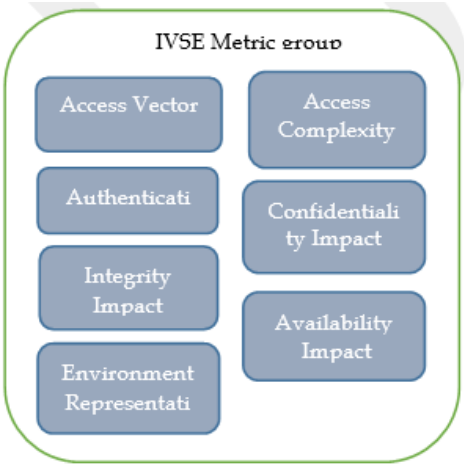


Fig.2. Base metric group of the Proposed IVSE

Proposed IVSE base score equation with environment representative

IVSE BS = Round_to_1_decimal(((0.5*Impact) + (0.3*Exploitability) + (0.2*Environment representative)-1.5)* f (Impact)

Impact=10.41 * (1- (1- Confidentiality Impact)*(1-Integrity Impact) * (1-Availability Impact))..... (1.0)

Exploitability=20 * Access Vector * Access Complexity * Authentication.....(1.1)

Environment Representative = 10*OE.....(1.2)

f(impact)= 0 if Impact=0, 1.176 otherwise.....(1.3)

2.2 Proposed IVSV (Improved Vulnerability scoring system with Vulnerability type)

Proposed IVSV is an improved vulnerability scoring technique with an additional factor "vulnerability type". Despite CVSS-v2 is a universal standard and accepted by numerous IT companies and individuals but after a detailed study it has been noticed that the "vulnerability type" should also be included as an essential factor in CVSS-v2 base score equation. It allows making a choice out of four common types of vulnerabilities. These four vulnerabilities are 'Authentication Weakness', 'Race Condition', 'Buffer overflow', and 'Unvalidated Input'. These vulnerabilities are found in normal coding process of software and seeks equal attention.Proposed IVSV is basically an improvement over CVSS-v2 base score equation. It contains an extra factor 'vulnerability type' into already available six factors of CVSS-v2 base group. Fig. 3 shows the Proposed IVSV base group.

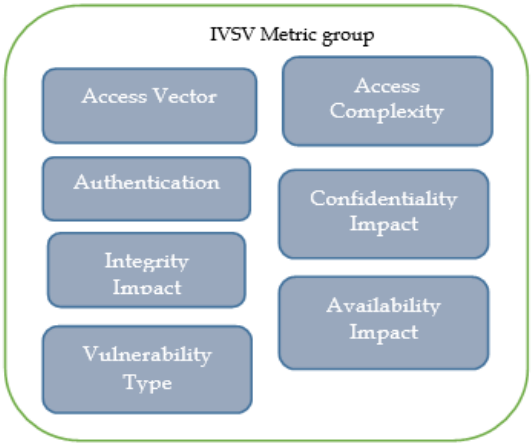


Fig.3. Base metric group of Proposed IVSV

Proposed IVSV base score equation with Vulnerability type

IVSV BS= Round_to_1_decimal (((0.5*Impact) + (0.3*Exploitability) + (0.2*Vulnerability type)-1.5)* f (Impact))..... (2.0)

Impact = 10.41 * (1-(1-Confidentiality Impact) * (1-Integrity Impact) * (1-Availability Impact)) ... (2.1)

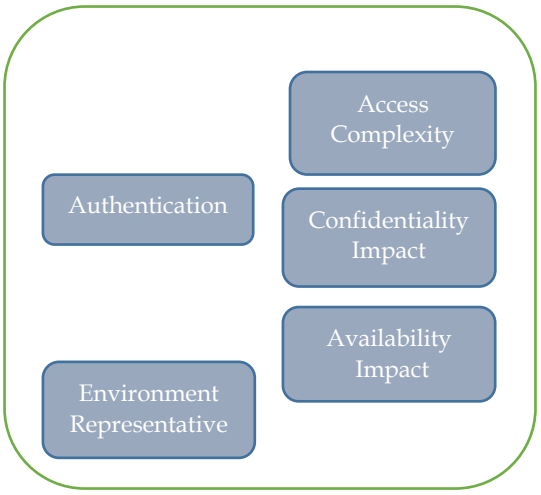
Exploitability = 20*Access Vector*Access Complexity*Authentication..... (2.2)

Vulnerability Type = 10*VC..... (2.3)

f(impact)= 0 if Impact=0, 1.176 otherwise..... (2.4)

3. IVSEV: Improved Vulnerability Scoring system with 'Environment Representative' and 'Vulnerability type'

Improvement in vulnerability scoring system is a never ending process. Number of Software, IT and other organizations are working for the betterment of scoring systems. In this section, we propose an improved scoring system IVSEV (Improved Vulnerability Scoring system with Environment representative and Vulnerability type). This system is basically an improvement over CVSS-v2 base score formula. Two new factors 'Environment representative' and 'Vulnerability type' are added into already available six CVSS-v2 factors.



Environment representative contains a metric group OE that reflects 'Operating Environment' of the user i.e. Linux/Windows/Mac and other operating systems. Impact of every vulnerability is different depending on the operating environment of affected user. Considering this an important point we added this factor into our proposed IVSEV system. Table 1. Shows the different operating environments.

Table 1
Operating environments of system

Metric type	Explanation	Metric Value
OE Type	Operating Environment of system	Linux/Windows/Mac and Others

"Vulnerability type" is also an essential aspect to be included into CVSS-v2 base score equation. Few common vulnerability types are 'Authentication weaknesses' 'Buffer overflow', 'Unvalidated Input' and 'Race condition'. The proposed IVSEV calculates the score by amending the conventional CVSS-v2 base score formula to accommodate the two new factors 'Environment representative' and 'Vulnerability type'. Fig. 4 shows the proposed IVSEV metric group.

Original CVSS-v2 base score equation

Base Score=round_to_1_decimal (((0.6*Impact) + (0.4*Exploitability)-1.5)*f(Impact)) ..... (3.0)

Impact=10.41*(1-(1-CI)*(I-II)*(I-AI) ..... (3.1)

Exploitability = 20*AV*AC*Au ..... (3.2)

f(impact)=0 if impact=0, 1.176 otherwise.....(3.3)

Equation 3.0, equation 3.1, equation 3.2 and equation 3.3 shows the original CVSS-v2 base score equations. In this AV refers to "Availability Vector", II refers to "Integrity Impact", CI refers to "Confidentiality Impact", and AI refers to "Availability Impact". The proposed IVSEV figure out the score by revising equation number 3.0

Proposed IVSEV Base Score Equation

IVSEV Base Score=round_to_1_decimal (((0.5*Impact) + (0.3*Exploitability) + (0.1*Environment representative) + (0.1*Vulnerability type) - 1.5) * f (Impact)) ..... (4.0)

Environment Representative = 10*OE..... (4.1)

Vulnerability Type = 10*VC..... (4.2)

f(impact)=0 if impact=0, 1.176 otherwise..... (4.3)

Equation 4.0 shows the modified base score equation with two new factors 'Environment Representative' and 'Vulnerability Type'. Weights of Environment representative and Vulnerability type are adjusted to 0.1 each. Hence the equation 4 of the proposed IVSEV gives weights 0.5 to Impact, 0.3 to exploitability, 0.1 to environment variable and 0.1 to vulnerability type variable. These weights are so assigned so as gives a sum of 1. The value for environment variable is calculated by equation 4.1 and value for vulnerability type variable is calculated by equation 4.2.

4. Results and Discussion

The proposed mechanism IVSEV is tested on sample set of

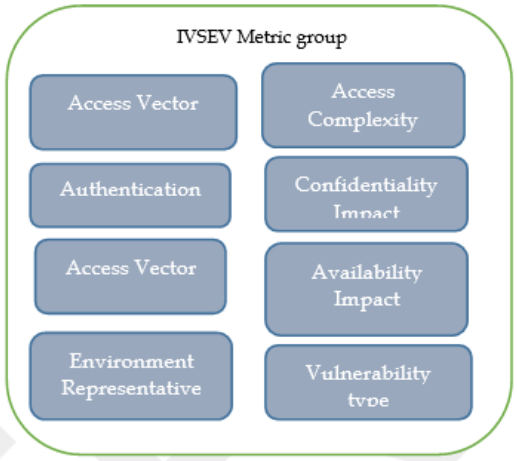


Fig.4. Base metric group of proposed IVSEV

vulnerabilities taken from NVD (National Vulnerability Database). NVD is a U.S. government project and one of the most relevant resources available online which helps the organizations and individuals to keep their software safe and secure. NVD includes databases of vulnerabilities, security-related flaws, impact metrics and misconfigurations. Table 2 show the scores resulted after including 'Environment representative' and 'Vulnerability type' into CVSS-v2 base score equation. Table 2 shows the CVSS-v2 base score for the given vulnerabilities and against these are shown the vulnerability scores computed with the proposed IVSEV under different host environment settings (Linux, Windows, Mac) and with different vulnerability types (BO, RC, UI, AW). For the same value of CVSS–v2 base score value for a given vulnerability the proposed IVSEV gives a set of 12 scores. These 12 scores generated depict different host environment and different vulnerability types. For every vulnerability for the given CVSS –v2 base score the proposed IVSEV score with AW vulnerability is mostly lower than CVSS-v2 base score in Linux and Windows host environment. In some vulnerabilities in MAC host environment the vulnerability score little more. For other vulnerability types as well like BO, RC and UI the scores with proposed IVSEV the scores vary as per the host environment and are different than the CVSS –v2 base score. Obtained results are then compared with conventional CVSS-v2 base scores.Hence, showing the severity of the vulnerability depending on the type of the vulnerability and the host environment in the proposed IVSEV base score itself. These two factors 'Environment representative' and 'vulnerability type' are important and needed in scoring the severity of the vulnerability. Whereas in CVSS–v2 these two factors are not considered in the base score and are optional. However, most of the vendors just refer the CVSS base scores only. Hence, the proposed IVSEV shows improvement in calculating base scores by including the two important factors viz. 'Environment representative' and 'vulnerability type' in its base scores.

Table 2
IVSEV Score resulted after adding ER and VT

Vulner-bility Number	CVSS -v2 score	IVSEV Score			
		Vulner-ty type	Host Environment		
			Linux	Windows	Mac
CVE-2018-20326	4.3	BO	4.8	4.5	5.1
		RC	4.6	4.2	4.8
		UI	4.4	4.0	4.6
		AW	4.2	3.9	4.5
CVE-2018-20166	6.5	BO	6.7	6.4	6.9
		RC	6.5	6.1	6.7
		UI	6.2	5.9	6.5
		AW	6.1	5.8	6.4
CVE-2018-17161	7.5	BO	7.4	7.1	7.7
		RC	7.2	6.8	7.4
		UI	7.0	6.6	7.2
		AW	6.8	6.5	7.1
CVE-2018-16171	6.8	BO	6.9	6.6	7.2
		RC	6.7	6.3	6.9
		UI	6.5	6.1	6.7
		AW	6.3	6.0	6.6
CVE-2018-4217	5.0	BO	5.3	5.0	5.6
		RC	5.1	4.7	5.3
		UI	4.9	4.5	5.1
		AW	4.7	4.4	5.0
CVE-2018-20650	4.3	BO	4.8	4.5	5.1
		RC	4.6	4.2	4.8
		UI	4.4	4.0	4.6
		AW	4.2	3.9	4.5
CVE-2019-7864	5.0	BO	5.3	5.0	5.6
		RC	5.1	4.7	5.3
		UI	4.9	4.5	5.1
		AW	4.7	4.4	5.0
CVE-2019-13024	9.0	BO	8.8	8.5	9.0
		RC	8.6	8.2	8.8
		UI	8.3	8.0	8.6
		AW	8.2	7.9	8.5
CVE-2019-4296	2.1	BO	3.2	2.8	3.4
		RC	3.0	2.6	3.2
		UI	2.7	2.4	3.0
		AW	2.6	2.3	2.8
CVE-2019-7296	4.3	BO	4.8	4.5	5.1
		RC	4.6	4.2	4.8
		UI	4.4	4.0	4.6
		AW	4.2	3.9	4.5

5. CONCLUSION

This research looked into the influence of adding 'Environment representative' and 'Vulnerability type' into CVSS-v2 base score equation. The proposed mechanism (IVSEV) is formed and examined on sample set of vulnerabilities retrieved from U.S. government repository (National Vulnerability Database). Obtained results with this new formula shows that both factors do make impact on scoring vulnerabilities. Table 3 shows the conventional CVSS-v2 base score formula and proposed IVSEV base score formula.

Table 3
CVSS and IVSEV base score equations

CVSS-v2	CVSS BS=round_to_1decimal (((0.6*Impact) + (0.4*Exploitability)-1.5)*f(Impact))
IVSEV	IVSEV BS=round_to_1decimal (((0.5*Impact) +(0.3*Exploitability)+(0.1*ER) + (0.1*VT) - 1.5) * f (Impact))

ER refers 'Environment representative' and VT refers 'Vulnerability type'.

6. REFERENCES

[1] Xinbo Ban, Shigang Liu, "A performance evaluation of deep-learnt features for software vulnerability detection" Wiley November 2018.
[2] Laurent Gallon, Mont de Marsan, "On the impact of environmental metrics on CVSS Scores" IEEE 2010 International Conference on Social computing.
[3] Akansha Rastogi, Kendall E. Nygard "Software Engineering Principles and Security Vulnerabilities" EPiC series in Computing, 2019.
[4] Saniora R. Duclervil, Jing-Chiou Liou "The study of the Effectiveness of the Secure Software Development Life Cycle Models in IT Project Management" Springer Nature Switzerland AG 2019
[5] Ruyi Wang, Ling Gao "An improved CVSS-based

vulnerability scoring mechanism" 2011 Third International Conference on Multimedia Information Networking and Security

[6] Ayodele Oluwaseun Ibidapo, Pavol Zavarsky "An Analysis of CVSS v2 Environment Scoring" IEEE 2011 International Conference on Social Computing.

[7] Georgios Spanos, Angeliki Sioziou "WIVSS: A New Methodology for Scoring Information Systems Vulnerabilities" PCI 2013.

[8] Gagandeep Chawla, Neeraj Sharma "IVSE: An Improved CVSS Base score mechanism with Environment representative" JETIR 2018.

[9] Gagandeep Chawla, Neeraj Sharma "IVSV: An Improved CVSS Base score mechanism with Vulnerability type" IJEAT 2019.

[10] Peter Mell, Karen Scarfone, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0" June 2007.