DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5380

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

TO STUDY AND ANALYZE THE IMPACT OF CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA) ON COMMON VULNERABILITY SCORING SYSTEM (CVSS) BASE SCORE

Deven Pandya
Ph.D. Scholar
Department of Computer Application,
Ganpat University
Kherva, Mehsana, Gujarat, India

Dr. N.J. Patel
Professor
Department of Computer Application,
AMPICS, Ganpat University
Kherva, Mehsana, Gujarat, India

Abstract: The Common Vulnerability Exposure (CVE) is a list of publically known vulnerabilities. The Common Vulnerability Scoring System (CVSS) is a benchmark vulnerability severity scoring system. The vulnerability severity score for vulnerability disclosed under CVE list is calculated using CVSS. The CVSS is calculated using three metrics viz. Base metric, Temporal metric, and Environmental metric. The base metric defines the basic characteristics of the vulnerability. The temporal metrics define the time-dependent characteristics of the vulnerability and the environmental metrics define the characteristics of the vulnerability specific to particular user's or organization's environment. The CVSS base score is available, in CVE dictionary and it can be refined by calculating and adding temporal and environmental metric score. In this paper, our objective is to compare and analyze the CVSS base score with an adjusted base score generated after adding user context requirement for CIA. To achieve this objective we have selected Google Android as a platform and apply CIA requirement in user context in various combinations of score viz. High, Low and Medium. The generated adjusted based score was analyzed and compared with existing base score to understand the impact of CIA on vulnerability severity score.

Keywords: Vulnerability; CVE; CVSS; Security Metric; CIA Triad

1. INTRODUCTION

The vulnerability is a weakness, bug, flaw or loophole in a system which can be exploited by threat actor to compromise the system. It is essential to have common standards for measuring vulnerability severity. The Security Content Automation Protocol (SCAP) is an amalgamation of interoperable security specifications.[1] SCAP is useful for automated vulnerability management, measurement, patch checking, configuration and policy compliance evaluation etc.[2] There are various specifications supported by SCAP for this purpose e.g. Common Platform Exposure (CPE) for asset management, Common Vulnerability Exposure (CVE), Common Vulnerability Scoring System (CVSS), Open Vulnerability Assessment Language (OVAL), Common Configuration Scoring System (CCSS) for Vulnerability Management and Extensible Configuration Checklist Description Format (XCCDF), Common Configuration Enumeration (CCE) for compliance management.[3] CVE is a list of publically known security vulnerabilities found in information systems. It is standard for Information Security vulnerability name.[4] The aim of the CVSS is to provide a common standard to incarcerate principal characteristics of the vulnerability and generate a numeric score to measure vulnerability severity in various information systems. The numeric severity score is translated into qualitative representation such as low, medium and high to facilitate organizations in prioritizing vulnerabilities in their information systems. [5]CVSS specification is available in different versions. Current CVSS version is version 3. In this article, we have utilized CVSS version 2 for the score calculation. The CVSS is calculated using Base metric, Temporal Metric, and Environmental Metric. Base metric represents the basic characteristics of the vulnerability which is invariable with the time and across user environment. The Access Vector, Access Complexity, and Authentication metrics define how the vulnerability is accessed, how many times the attacker needs to authenticate for a successful attack and in case any additional condition is required to exploit the vulnerability. Apart from this Impact metrics measures the impact of the attack on three CIA triad viz. Confidentiality, Integrity, and Availability if vulnerability exploited by the attacker. Temporal metric represents the characteristics of the vulnerability which may vary over time. It includes an affirmation of technical particulars of the vulnerability, remedial status of the vulnerability and code or techniques available for exploiting the vulnerability. The environmental metric group represents the vulnerability traits that are related to a user's IT environment. It includes collateral damage prospective, target distribution, and Confidentiality, Integrity, and Availability (CIA) condition metrics. Collateral damage metric measures the probable loss of asset or life, harm or pilfering of property and monetary loss of productivity or revenue. Target distribution is calculated as the percentage of the system affected by the vulnerability. Requirement metrics helps the organization to prioritize the vulnerability by adjusting the base score according to the importance of asset by adjusting CIA impact on the asset as per user environment. The more detailed specification is given in CVSS specifications guide available on FIRST-Forum of Incident Response and Security Team website.[6] It is necessary to prioritize vulnerability in order to prioritize the risk and its impact generated by the successful exploitation of the given vulnerability. As per the CVSS specification document, we can refine vulnerability scoring by adding temporal an environmental score. This will add context to the vulnerability severity score and it results in a more accurate reflection of the risk posed by the vulnerability in user context. Our objective is to compare available base score results with adjusted base score results by adding confidentiality, integrity, and availability (CIA) requirement in user or organization context and analyze the available results. To achieve our objective we have chosen vulnerability list pertaining to Google Android as a case and obtained a base and temporal score for Google Android vulnerabilities. After obtaining base score we have calculated the adjusted base score by applying permutation combination of CIA requirement in user or organization context. For final analysis vulnerability frequency in each severity category viz. High, Low and Medium are compared with vulnerability frequency of adjusted based score. The remaining paper organized in two sections methodology and conclusion.

2. METHODOLOGY

There is a large user base for Android Smartphone worldwide. As per CVE list number of distinct vulnerabilities found in android for the year 2017 is highest in top 50 products and hence it is a clear choice to use as a case for demonstrating the effect of adding individual user's confidentiality, availability, and integrity requirement information in the CVSS calculation. We have utilized CVSS specification version 2 in this paper for score generation. There are total 692 vulnerabilities in Google Android as on October 2017 as per the CVE list. Out of these 692 vulnerability entries, we have considered vulnerability entries made public in the year 2017 or CVE ID assigned to the vulnerability in the year 2017. [7] With this criterion we are left with only 447 vulnerability entries after removing vulnerability entries assigned with CVE ID in a year other than 2017. After downloading CVE list with the base score and all representative metrics value of the CVSS base score we have collected temporal score values with their representative metric values from the IBM X-force Exchange database. IBM X-force exchange is cloud platform for threat intelligence sharing and collaboration among users' and researchers' interested in cybersecurity.[8] Out of 447 vulnerabilities, we have found the temporal score for 440 vulnerabilities with the values for report confidence, remediation level, and exploitability hence for our study purpose we have to consider 440 vulnerability entries related to Google Android for the year 2017. We have utilized following equations obtained from CVSS v2 specification for calculating the base score and temporal score.

Base_Score = Round_One_Decimal[[{(0.6*CIAImpact) + (0.4* Exploitability)-1.5} * f_Impact]] (1)

Base_Score value is depend upon impact and exploitability metrics hence

CIAImpact = 10.41*[1-(1-Conf_Impact)*(1-Integ_Impact) *(1-Avail_Impact)] (2)

Exploitability=20* Access_Vector* Access_Complexity *Authentication (3)

f_impact= 0 if CIAImpact=0, 1.176 otherwise

The temporal metrics is calculated based on Base_Score value, exploitability, remedial status and report confidence metrics hence

Temp_Score=Round_One_Decimal[[Base_Score* Exploitability *Remedial status * Report Confidence]] (4)

After calculating temporal score we want to calculate environmental metric score based on following equation.

Env_Score=Round_One_Decimal[[(AdjustedTemp_Score + (10-AdjustedTemp_Score) *Collateral_Damage_Potential)*Target_Distribution]] (5)

Environmental Score will be calculated based on the adjusted temporal score. The adjusted temporal score will be calculated based on the adjusted based score. The adjusted based score will be calculated using adjusted CIA impact as given in below equation.

AdjustedCIAimpact = min[10,10.41*(1-(1-Conf_Impact * Conf.Req)* (1-Integ_Impact * Integ.Req * (1-Avail_Impact* Avail.Req))] (6)

For the scope of this study, we consider collateral damage potential and target distribution value as zero since our objective is the calculation of adjusted impact score and zero value for these two metrics do not affect the calculation. For the calculation of adjusted impact score, we tried a different combination of high and low values for confidentiality, integrity, and availability. We have not considered medium value since it is the default value and does not affect the score. We have applied eight permutation combinations considering it as eight different group of user environment as shown in below Table I for calculating the adjusted base score. The high and low is represented by values 1.51 and 0.50 respectively.

Table I

Group	Confidentiality	Integrity	Availability
GR1	1.51	1.51	1.51
GR2	1.51	1.51	0.5
GR3	1.51	0.5	1.51
GR4	1.51	0.5	0.5
GR5	0.5	1.51	1.51
GR6	0.5	1.51	0.5
GR7	0.5	0.5	1.51
GR8	0.5	0.5	0.5

Based on above value and using equation 6, we calculated adjusted impact score for all 440 vulnerability entries. Using obtained adjusted impact score and replacing adjusted impact score in equation 1, we have obtained adjusted based score for all vulnerability entries and all eight groups. As per CVSS, V2 document vulnerability is grouped according to its severity score. The vulnerability severity is divided into three categories as per the document viz. High with all vulnerabilities having severity score between 7 to 10, Medium with all vulnerabilities having severity score between 4 to 6.9 and Low with all vulnerabilities having severity score between 0 to 3.9. Following Table II depicts the number of vulnerabilities found in each of these categories using the base score and adjusted based score with eight different confidentiality, integrity and availability requirement values in the user environment. Table III depicts the same values in percentage form for a clear understanding of impact. The percentage was obtained out of total 440 vulnerability entries. From the Table III, we have prepared stacked bar chart as given in chart1 to understand the contribution of each category in overall base score severity.

Table II

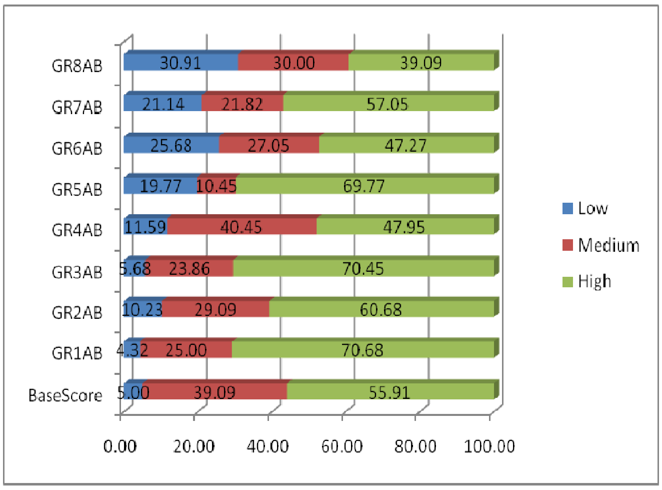
Group	Low	Medium	High
GR1-Adjb	19	110	311
GR2-Adjb	45	128	267
GR3-Adjb	25	105	310
GR4-Adjb	51	178	211
GR5-Adjb	87	46	307
GR6-Adjb	113	119	208
GR7-Adjb	93	96	251
GR8-Adjb	136	132	172
Base Score	22	172	246

Table III

Group	Low	Medium	High
GR1-Adjb	4.32	25.00	70.68
GR2-Adjb	10.23	29.09	60.68
GR3-Adjb	5.68	23.86	70.45
GR4-Adjb	11.59	40.45	47.95
GR5-Adjb	19.77	10.45	69.77
GR6-Adjb	25.68	27.05	47.27
GR7-Adjb	21.14	21.82	57.05
GR8-Adjb	30.91	30.00	39.09
Base Score	5.00	39.09	55.91

Below given stacked bar chart depicts the contribution of each severity category in the total number of vulnerability in each group.

Chart I



From the above Chart I, we have derived following Table IV depicting increase or decrease in a number of vulnerabilities in each group in comparison to base group.

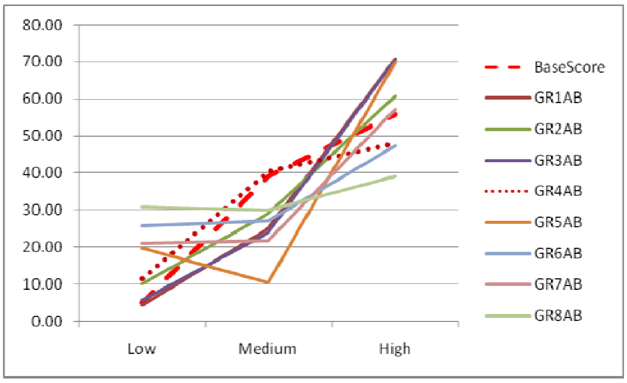
Table IV

Group	Low	Medium	High
GR1-HHH	Marginally Reduce	Reduce	Increase
GR2-HHL	Marginally Increase	Reduce	Increase
GR3-HLH	Marginally Increase	Marginally Reduce	Increase
GR4-HLL	Marginally Increase	Marginal Increase	Marginal Reduce
GR5-LHH	Increase	Reduce	Increase
GR6-LHL	Increase	Reduce	Marginal Reduce
GR7-LHH	Increase	Reduce	Marginal Increase
GR8-LLL	Increase	Marginal Reduce	Reduce

In the above Table VI, we have considered marginal increase or decrease for +/- 10% difference from base score. From the above table, we have deduced following facts related to vulnerability severity calculated using CVSS base metric and impact of confidentiality, integrity, and availability in the user context on CVE base score.

- The number of vulnerabilities in high severity category is increasing in case confidentiality requirement is high and other two requirements, integrity and availability is either both high and one is high and other is low.
- The number of vulnerabilities in low severity category is increasing in case confidentiality requirement is low and other two requirements integrity and availability is either both low and one is high or other is low.
- The number of vulnerabilities in the medium category is either shifting to high severity category or low severity category except in a group 4 where confidentiality requirement is high and other two requirements viz. integrity and availability are low.
- The number of vulnerabilities in each severity category in the base score is nearly equal to a number of vulnerabilities in each severity category in group 4 where confidentiality requirement is high and other two requirements viz. integrity and availability is low since there is a marginal difference in number of vulnerabilities in each severity category in group 4 and base score. The same is depicted using a line chart as given below where we can clearly see that base score and group 4 line is in close proximity to each other and there is a marginal difference in between these two lines towards the start and end.

Chart II



3. CONCLUSION

From the above study, we can deduce that there is a significant impact on the base score when we add user context values such as confidentiality, integrity, and availability requirement in CVSS base score calculation to generate an adjusted base score. The adjusted based score is more authentic and reflects the current user needs in terms of confidentiality, integrity, and availability of their information asset. There is a significant impact of confidentiality on vulnerability severity score as seen from results of group 1 to group 3 where vulnerability with high severity increased due to high confidentiality and in case of group 5 to 8 low severity is increased due to low confidentiality requirement. Apart from this number of vulnerability in each group viz. high, low, medium remains almost equal to the number of vulnerabilities in each group viz. high, low, medium in the base score when confidentiality is high and other two viz. integrity and availability is low. These are the results of the adjusted base score calculated using adjusted impact of confidentiality, integrity, and availability requirement in CVSS score of vulnerabilities given in CVE list for android platform. As a future research one can take any other software platform and check the impact of confidentiality, integrity, and availability requirement to generate the adjusted base score and generate results in a similar pattern as given above. The ultimate aim is to depict the impact of CIA on vulnerability score and identify the group which gives vulnerability score similar to the base score.

REFERENCES

[1] SCAP-NIST. [Online]. https://scap.nist.gov/

[2] Beyond Trust Blog. [Online]. https://www.beyondtrust.com/blog/a-basic-guide-to-scap/

[3] A. STACHURSKI RR. KASPRZYK, "A concept of standard-based vulnerability management automation for
IT systems," Computer Science and Mathematical Modelling, no. 3, pp. 33-38, 2016.

[4] CVE MITRE Corporation. [Online]. https://cve.mitre.org/

[5] FIRST SIG. [Online]. https://www.first.org/cvss/

[6] FIRST Website. [Online]. https://www.first.org/cvss/v2/guide

[7] CVE List. [Online]. https://www.cvedetails.com/top-50-products.php?year=2017

[8] IBM X-Force Exchange. IBM X Force Exchange. [Online]. https://www.ibm.com/security/xforce/