# Information Security Assessment by Quantifying Risk Level of Network Vulnerabilities

Umesh Kumar Singh
Institute of Computer Science
Vikram University Ujjain, M.P.
India

Chanchala Joshi
Institute of Computer Science
Vikram University, Ujjain, M.P.
India

Neha Gaud
Institute of Computer Science
Vikram University, Ujjain, M.P.
India

## ABSTRACT
With increasing dependency on IT infrastructure, the main objective of a system administrator is to maintain a stable and secure network, with ensure that the network is robust enough against malicious network users like attackers and intruders. Security risk management provides way to manage the growing threats to infrastructures or system. This paper proposes a framework for risk level estimation that uses vulnerability database National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS). The proposedframework measuresthe frequency of vulnerability exploitation; converges this measured frequency with standard CVSS score and estimates the security risk levelwhich helps in automated and reasonable security management. In this paper, equation for the Temporal score calculation with respect to availability of remediation plan is derived and further, frequency of exploitation is calculated with determined temporal score. The frequency of exploitation along with CVSS score is used to calculate the security risk level of the system. The proposed framework uses the CVSS vectors for risk level estimation and measures the security level of specific network environment, which assists system administrator for assessment of security risks and making decision related to mitigation of security risks.

## Keywords
CVSS metrics, risk level, security measurement, severity score, vulnerability category.

## 1. INTRODUCTION
With the growth of information system most of our everyday activities depend on services provided by computer networks. So, the primary objective of a system administrator is to maintain a reliable network, with ensure that the network is robust enough against malicious network users like attackers and intruders. Security risk management provides way to manage the growing threats to infrastructures or system. Vulnerability management is essential for mitigation of security risks. It has to be proactive and increasingly automated to ensure that vulnerabilities are assessed, prioritized and remediated speedily before they are located and exploited. The Common Vulnerability Scoring System allows to rate, compare and understand the importance of different vulnerabilities and thus to prioritize them. CVSS was first released for public use in 2004 with the goal of vulnerability prioritization [1]. CVSS allocates a severity score to each vulnerability. This score helps to measure the potential danger of the vulnerability for the organization in which it is detected. Calculation of CVSS score considers the intrinsic characteristics of vulnerability (Base vector), its evolution over time (Temporal vector) and security level of organization (Environmental vector). Each vector is composed of several metrics that must evaluate in order to compute corresponding CVSS score. All Base metrics must be included in CVSS score while Temporal and Environmental metrics are optional. This paper focuses on the part of CVSS score which concerns the duration of exploitation (Temporal vector) and the security level of the organization (Environmental vector). The objective is to analyze the impact ofTemporal vector and Environment vector on the CVSS score. The methodology begins with the study of CVSS score of one of the vulnerability database National Vulnerability Database (NVD) [2] because these score represent the intrinsic characteristics of vulnerability (Base metrics). Then modified CVSS score is calculated by stimulating all possible values of environment metrics. Finally, result is analyzed for security risk evaluation.

## 2. RELATED WORK
Some work has already done in the field of vulnerability prioritization to estimate risk level. Tripathi and Singh [3] proposed a security metrics to prioritize vulnerability categories based on CVSS scores. The metrics is further applied on 5177 vulnerabilities extracted from NVD published in recent one year and vulnerability categories are prioritized and ranked based on cumulative severity scores. [4][5] discussed the security trade-off analysis to measure the risk level accurately. Tripathi and Singh [6] evaluated vulnerabilities protection by calculating a metric based on a number of factors like the number of vulnerabilities present in the system, vulnerability discovery date and their exposure to the network and traffic patterns and estimated risk level of NVD vulnerability categories based on vulnerability characteristics, distribution of vulnerability and age of vulnerability. Joshi et al. [7] evaluated the efficiency of web application vulnerability scanners by designing a vulnerable web application. Also, some defense measures are suggested to secure the application and to improve scanner's detection rate. In [8] prominent taxonomies of attacks and vulnerability of computer system and network are reviewed to improve vulnerability categorization. In [9] Joshi et al. proposed an approach towards Standardization of Network and Computer Attack Taxonomies. Sawillaet al. [10] used two attributes from the CVSS for vulnerability prioritization under the perspective of attackers. However, instead of using the rating values directly from the CVSS they used their own values.

## 3. VULNERABILITY DATABASE
Proposed method to evaluate severity index of vulnerability begins with study of vulnerability database. So, this subsection presents an overview of one of the vulnerability database National Vulnerability Database (NVD). The vulnerabilities in NVD are based on the Common Vulnerabilities and Exposures (CVE) vulnerability-naming standard and are organized according to severity, determined

by the Common Vulnerability Scoring System (CVSS) standard. The CVE list [11] an initiative to standardize vulnerability references and gives vulnerabilities a name in the form CVE-YYYY-XXXX, where YYYY is the year, in which the vulnerability is first reported. This central database allows each of the vulnerabilities to have one unique identifier, a CVE id, such as "CVE- 2016-3649". CVE is actually a dictionary of vulnerabilities than a database[14]. For determining the severity of computer security risks, the National Vulnerability Database (NVD) is one ofNIST's important security assets. NVD is the combination of many other security databases allowing the fullest utilization of available public computer security risk analysis and quantification methods via CVSS scores [12]. NVD is also linked with CVE to enable comparison and expansion of NVD with CVE entries. NVD records vulnerabilities since 1999, total 77060 vulnerabilities listed under CVE names till May 4, 2016 [13]. There are total 23 types of vulnerability in NVD classification scheme. NVD provides extensive searching under various categories; published date range, last modified date range and under different CVSS base metric parameter values. NVD uses CVSS scores to define severity of vulnerability. CVSS (Common Vulnerability Scoring System) is used to quantify the severity of a vulnerability to an information system. It was designed by FIRST (Forum of Incident Response and Security Teams) in 2004. [14] NIST NVD is prominent security assets for measuring the severity of vulnerability. NVD uses CVSS for quantitative security risk analysis. One can derive vulnerability blueprint using the NVD's information about vulnerability; this derived blueprint can used to calculate the severity score of identified vulnerabilities in organization's network configuration. NVD contains an openly available resource that provides valuable information for measuring the severity of computer security risks.

# 4. COMMON VULNERABILITY SCORING SYSTEM

The Common Vulnerability Scoring System (CVSS) provides an open framework for measuring severity of vulnerabilities. CVSS contains three metric groups: Base metric group, Temporal metric group and Environmental metric group. [15] The Base group reflects the intrinsic properties of vulnerability, the Temporal group represents the dynamic behavior of a vulnerability that changes over time, and the Environmental group defines the unique user's environment characteristics of a vulnerability. The Base metrics generate a score ranging from 0 to 10. This numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Following figure shows the architecture of CVSS metrics group [15]:

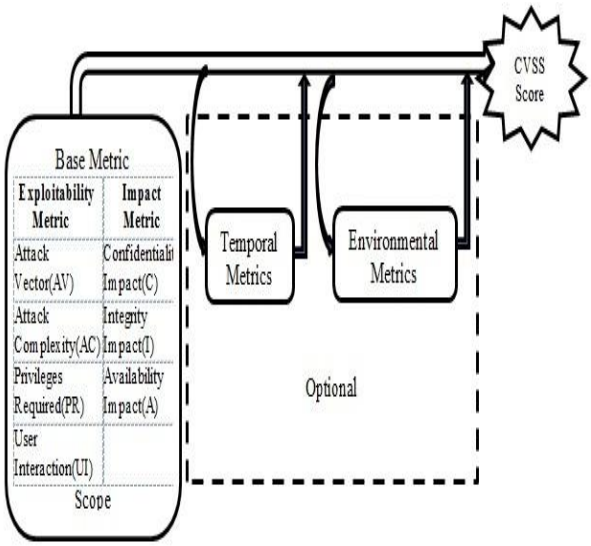


**Figure-1: CVSS Metric Groups**

## 4.1 Metrics

The Base metric group represents the intrinsic characteristics of vulnerability that are constant over time and across user environments[15]. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.

The Exploitability metrics represent the characteristics of vulnerable component by which vulnerability can be exploited. Whether, the Impact metrics represent the consequence on to the impacted componentfor sucessful exploit.The Temporal metric group represents the dynamic behavior of vulnerability. The Environmental metric group represents the user's environment properties of vulnerability. These metrics help the scoring analyst to implement security controls [15], that may mitigate any consequences, as well as promote or demote the importance of a vulnerable system according to business risk.

## 4.2 Vulnerability Severity Scale for Qualitative Rating

To help organizations properly assess and prioritize their vulnerability management processes the CVSS numerical score can then be translated into atextual qualitative representation [15]:

**Table 1. Vulnerability Qualitative Severity Rating Scale**

| Rating | CVSS Score |
|---|---|
| None | 0.0 |
| Low | 0.1 to 3.9 |
| Medium | 4.0 to 6.9 |
| High | 7.0 to 8.9 |
| Critical | 9.0 to 10.0 |

These qualitative severity ratings help organizations in properly assessessment and prioritizationduring vulnerability management processes.

## 4.3 CVSS Equations

Proposed CVSS scoring scheme primarily uses CVSS Base Score, therefore, understanding the Base equation is the first step of proposed methodology. The Base Score is a function of the Impact and Exploitability sub score equations[15].

*Where the Base score is defined as,*

*If impact=0 thenBase Score=0*

*Else Scope Unchanged Roundup (Minimum [(Impact + Exploitability),10])*

*Scope Changed Roundup (Minimum [1.08 × (Impact + Exploitability),10])*

*And Impact can be defined as*

*Scope Unchanged* $6.42 \times ISC_{Base}$

*Scope Changed* $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

*Where,* $ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Intea}) \times (1 - Impact_{Avail})]$

*and Exploitability can be defined as*

*PrivilegeRequired × UserInteraction*

All the above equations are defined in CVSS v3.0 specification document [15].

## 4.4 Standard Quantitative Risk Models

Ahmed et al. [18] proposed a framework for quantitative risk level measurement that measures the security risk of a network mainly on two prominent risk aspects - the risk of having a successful attack and the risk of this attack being propagated within the network. Another prominent framework for risk level measurement is proposed by Tripathi et al. [3] that estimates risk level of NVD vulnerability categories based on vulnerability characteristics, distribution of vulnerability and age of vulnerability. We have, therefore, modeled our framework as a combination these two with the aid of Environmental factor. Tripathi et al. [3] introduced Temporal factor, considering age of vulnerability is a prominent factor that can impact security risk level. This paper is also considering the aging factor; however, we redefine it as maturity of exploit. Equations for calculating Temporal score are also redefining in this paper with respect to availability of patch. With the addition of Temporal factor, this paper uses Environmental factor which contains the frequency of exploit in user's environment. In proposed model Base score of CVSS is updated by applying temporal score and environmental score of vulnerability. The next section will describe the proposed improved quantitative security risk level estimation model in detail.

# 5. PRAPOSED FRAMEWORK FOR QUANTITATIVE SECURITY RISK LEVEL ESTIMATION

In security management, quantifying security risk is an important and challenging task for securing the network proactively. However, there are metrics exist to measure risk level of individual vulnerabilities [17] but to aggregate these risk values to evaluate risk level of host there is no standard matrix available. To evaluate risk level of host in a network (user's environment) by aggregating risk levels of vulnerabilities (intrinsic properties of vulnerability), this paper re-organize the CVSS score by stimulating the maturity of exploit code with respect to remediation plan and frequency of exploit code. In figure 2 the proposed Quantitative Security Risk Level Estimation Model is shown. In proposed model, risk level of vulnerability categories estimated based on intrinsic characteristics of vulnerabilities, frequency of vulnerability and maturity of the vulnerability with respect to availability of patches.

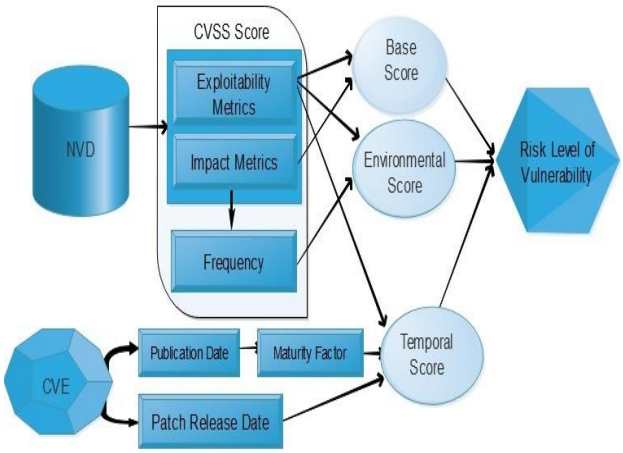


**Figure-2: Proposed Quantitative Security Risk Level Estimation Model**

In the proposed model to define vulnerability characteristics, CVSS Base metrics: exploitability metrics and impact metrics are used. These two metrics groups in include three individual metric values in each, Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR) and User Interaction(UI) are associated with Exploitability Metrics and Confidentiality Impact (C), Integrity Impact (I), Impact (A) are associated with Impact Metrics. So, all these nine attributes are used to characterize vulnerability. Base value for vulnerability category risk level is evaluated from value of each of these attributes and frequency of vulnerabilities in various combinations of these attributes.

To reflect change in risk level with time, temporal score is calculated. In proposed methodology Temporal score is calculated by convergence of maturity of vulnerability with availability of patches. Maturity score is determined by the date of emergence of vulnerability and availability of patches is discovered by Remediation Level (RL) vector of CVSS metrics.

The more frequent occurrences of vulnerability make system riskier; so by keeping this assumption the proposed model introduced a new dimension to the available standard Quantitative risk model, the Environmental metrics, which is used to estimate the frequency of vulnerability. The assumption behind frequency computation is that a highly exploitable vulnerability is more likely to be misused by attackers and consequently should have a higher frequency. Hence, for frequency calculation Attack Vector (AV), Attack Complexity (AC) and Privileges Required (PR) attribute of Base Metrics of CVSS are used by which we can determine the exploitability of vulnerability. Frequency of vulnerability also depends on the period of presence of vulnerability in the system, so the exploitability attributes are combined with temporal score for frequency estimation. For computation of risk level, the base risk score is updated by applying temporal score and environmental score of vulnerability. This evaluated risk level value will be used in evaluation of severity of vulnerabilities.

## 5.1 Computations of risk level

The proposed Quantitative CVSS Risk Level Estimation Model follows four steps computational procedures:

Step 1: Computation of Base score using intrinsic properties of vulnerability by CVSS Base score equation.

Step 2: Computation of Temporal Score using maturity of exploit with respect to availability of patch.

Step 3: Estimation of frequency of exploit by Base Metrics, Temporal Metrics and Environment metrics of CVSS.

Step 4: Derive risk level from estimated maturity and frequency.

Computation of Base score in Step 1 involves the identification of both the vulnerabilities and capability of exploiting the vulnerabilities. CVSS Base score equations described in previous section '4.3' are used for the Base score computation. Computation of Temporal score involves two sub steps, at first maturity of exploit will be calculated by date of emergence of vulnerability, and then this maturity will be simulated by availability of patch. Availability of patch can be determined by Remediation Level (RL) and Report Confidence (RC) factor of CVSS [15]. Attack Vector (AV), Attack Complexity (AC) and User Interaction (UC) attribute of Base Metrics of CVSS and Temporal score computed in step 2 are used for frequency estimation of vulnerability. Finally, the risk level will be computed from Base score, Temporal score and frequency, computed in previous three steps.

Estimation of frequency and computation of Temporal score is described briefly in the next section '5.2'.

## 5.2 Enhancing CVSS by frequency and maturity estimation

CVSS defines the severity of vulnerability. But the severity of a vulnerability depends not only on the intrinsic characteristics of vulnerability (i.e. Base score). Besides the CVSS scores there are many more factors that control the severity level of vulnerabilities, like remediation level of vulnerability, maturity of exploit code. With these vectors, the risk level of vulnerability can be defined.

The maturity of vulnerability can be determined by the date of emergence of vulnerability, from NVD. This maturity score combines with availability of patches to further define the impact of vulnerability. Remediation Level (RL) vector of CVSS signifies the availability of patches. For estimation of risk level, it is assumed that vulnerabilities that are discovered recently and have no patches available cause more security risks as compared to vulnerabilities that have patches available. Over the time user patch these vulnerabilities so with the time severity level of vulnerability decreases.

CVSS metric groups consist of a set of attributes, these attributes with Time score are used to estimate the frequency in Step 3 of the computational procedure specified in previous section. The assumption behind frequency computation is that a highly exploitable vulnerability is more likely to be misused by attackers and consequently should have a higher frequency. By considering the intrinsic exploitability factors of the vulnerability itself (i.e., the base metric attributes relevant to exploitability) and the temporal score; it is possible to calculate the exploitability frequency of vulnerability present in a system. The next subsection describes the estimation of maturity and frequency that aids in risk level estimation.

### *5.2.1 Estimation of temporal score*

Temporal score of vulnerability is depending on two factors, availability of patches and maturity of exploit code. Maturity can be determined by emergence date of vulnerability, taken from NVD. Convergence of the maturity score with availability of patches, the impact of vulnerability can be defined. Considering these factors metric formulae are developed to evaluate temporal score for vulnerability. To calculate temporal score, vulnerabilities are divided into two categories, for which patches are not available, and for which those have patches available. We calculate RemediationLevel in these two types separately and then Temporal Score will be calculated as

$$Temporal\ Score = BaseScore \times (1/RemediationLevel) \times MaturityOfExploitCode$$

Here we are taking reciprocal of Remediation Level (RL) vector because the value of RL is higher for high severity vulnerability than the vulnerability having medium or low severity.

Temporal score is based on the assumption that vulnerabilities that are discovered recently and have no patches available cause more security risks as compared to vulnerabilities that have patches available. Over the time user patch these vulnerabilities so with the time severity level of vulnerability decreases.

### *5.2.2 Estimation of frequency of vulnerability from CVSS metrics*

Attack Vector (AV), Attack Complexity (AC) and Privileges Required (PR) attribute of Base Metrics of CVSS and Temporal score computed in previous step are used for frequency estimation of vulnerability.

$$Frequency = (AV*AC*PR) + Temporal\ Score$$

The Base metric attributes refer intrinsic property of vulnerability, while the temporal score attributes describe dynamic behavior of vulnerability in user's environment. For this reason, the Base metric attributes are used to establish an initial frequency value which is further updated using the temporal score.

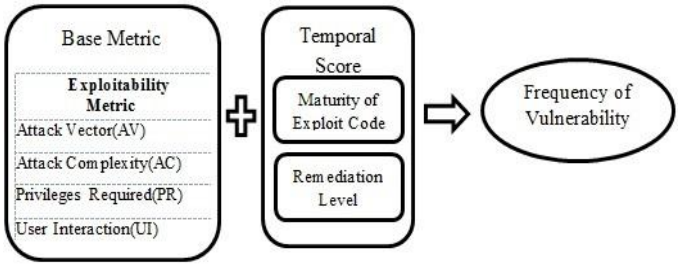


**Figure-3: Frequency estimation from CVSS Base Metric and Temporal Score**

CVSS metric groups consist of a set of attributes, these attributes with Time score are used to estimate the frequency.

Following table summarizes the CVSS attributes relevant for the calculation of frequency estimate [15]:

**Table 2. CVSS attribute values for frequency estimation**

| Metric | Metric Value | Numerical Value |
|---|---|---|
| Attack Vector | Network | 0.85 |
| | Adjacent Network | 0.62 |
| | Local | 0.55 |
| | Physical | 0.2 |
| Attack Complexity | Low | 0.77 |
| | High | 0.44 |
| Privilege Required | None | 0.85 |
| | Low | 0.62 |
| | High | 0.27 |

The assumption behind frequency computation is that a highly exploitable vulnerability is more likely to be misused by attackers and consequently should have a higher frequency. By considering the intrinsic exploitability factors of the vulnerability itself (i.e., the base metric) and the temporal score; it is possible to calculate the exploitability frequency of vulnerability present in a system.

### *5.2.3 Risk level Computation Equation*

As we have assumed that the more frequent occurrences of vulnerability make system riskier; i.e. Risk level of the system also depends on the frequency of vulnerability. With this assumption, the proposed Quantitative Risk Level Evaluation model converges frequency of vulnerability derived in the previous section with the CVSS score, for Risk Level estimation of the system. Therefore, for risk level evaluation we sum up the frequency and CVSS Score of the vulnerability:

$$Risk\ Level = (Minimum\ [(CVSS\ Score + Frequency),10])$$

In proposed methodology, we are considering the range of risk level in between 0.0 to 10.0. Therefore, if the sum of CVSS score and frequency is more than 10, then the value of risk level is taken as 10. For this we are applying minimum function to the proposed equation, that will return 10 if sum is more than 10.

## 6. APPLYINGTHE PROPOSED MODEL ON TO THE STANDARD CVSS SCORE FOR RISK LEVEL ESTIMATION

As described in Section '5.1' Step 1 of the computational procedure of the CVSS Risk Level Estimation Model focuses on identifying intrinsic properties of vulnerabilities by Base score. We examined vulnerability databases NVD to check for recently released vulnerabilities. The Step 1 activity resulted in more than 20 potential vulnerabilities published during April to July 2016. CVSS Base score of these vulnerabilities is taken from NVD, as NVD contains the information about vulnerability's CVSS Base score. The CVSS score defines the severity of vulnerability. Besides the severity of vulnerability, the two major factors that affect system's security and can increase risk level of system failure are, the maturity of vulnerability and the frequency of vulnerability. So, in the next steps the estimation of these two factors is done and finally the risk level will be evaluated. We are taken "CVE-2016-3092" vulnerability to elaborate our proposed methodology. The step 2 of the computational procedure concerns estimating the Temporal Score of the vulnerabilities identified in Step 1. Temporal score equation defined in previous section uses maturity of vulnerability and Remediation Level vector of CVSS. The value of RemediationLevel vector is computed by using CVSS v3 calculator [19] and maturity is determined by the Published date of vulnerability taken from NVD. With Base score, RemediationLevel vector and maturity of vulnerability we are calculating the Temporal score.

$$Temporal\ Score = BaseScore \times (1/RemediationLevel) \times MaturityOfExploitCode$$

RemediationLevel of CVE-2016-3092 vulnerability is 0.7(by CVSS3.0 calculator) and maturity is 16 days on 20 July 2016. The maturity of vulnerability is considered as 1 because average patch release time for vulnerability ranges in 23 to 40 days[6].

Hence, Temporal score = 7.8 * (1/14.28) * 1

⇨ Temporal score = 0.546

In Step 3, frequency of the CVE-2016-3092 vulnerability estimated according to the CVSS metric attributes using the equation described in previous section:

$$Frequency = (AV*AC*PR) + Temporal\ Score$$

Temporal score calculated in previous step is 5.46.The CVSS information available in the NVD for the vulnerability CVE-2016-3092 published on 2016-07-04 is as follows:

Attack Vector (AV): Network

Attack Complexity(AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): None

Integrity (I): None

Availability (A): High

With these identified factors we can calculate the frequency of vulnerability CVE-2016-3092.

Hence, Frequency= (AV*AC*PR) + Temporal Score

⇨ Frequency= (Network*Low*None) + 0.54

⇨ Frequency= (0.85*0.77* 0.85) +0. 54

⇨ Frequency=0.55 + 0.54

⇨ Frequency=1.09

With these calculated factors, vulnerability severity, maturity and frequency the risk level of vulnerability is evaluated. For risk level evaluation we sum up the frequency and CVSS Score of the vulnerability:

*Risk Level = (Minimum [(CVSS Score + Frequency),10])*

We defined the range of risk level in between 0.0 to 10.0.

# 7. QUANTITATIVE RISK EVALUATION

For risk evaluation, we are considering 25 potential vulnerabilities published during April to July 2016. Maturity scores, frequenciesand risk levels of these vulnerabilities are calculated using proposed methodology shown in the table 3.

The table contains the following data:

1) The first column represents the serial number.
2) The second column contains CVE-ID of vulnerability.
3) Third column contains the CVSS score of vulnerability computed using Base score of CVSS Metrics.
4) Fourth column represents the emergence date of vulnerability, which is taken from NVD.
5) Fifth column shows the qualitative severity level of vulnerability derived by CVSS score (defined in table 1).
6) Sixth column shows the availability of patch up to date 2016-07-21; 'Y' entry in this column indicates that patch is available while we put 'N' if the patch is not available.
7) Seventh column computed maturity score till 2016-07-21 with respect to published date.
8) Eighth column represents the frequency of vulnerability calculated using proposed model.
9) Ninth column represents the risk level determined by frequency, maturity of exploit and severity score.

**Table 3. Quantitative Risk Level Evaluation**

| **SN** | **CVE-IDs** | **CVSS Score** | **Published Date** | **Severity** | **Patch Availability** | **Maturity on** 2016-07-20 (In days) | **Frequency** | **Risk Level** |
|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2015-6360 | 7.8 | 2016-04-21 | High | Y | 89 | 0.43 | 8.23 |
| 2 | CVE-2014-9761 | 7.5 | 2016-04-19 | High | N | 91 | 1.02 | 8.52 |
| 3 | CVE-2015-8778 | 7.5 | 2016-04-19 | High | Y | 91 | 0.12 | 7.62 |
| 4 | CVE-2015-8779 | 7.5 | 2016-05-19 | High | Y | 91 | 0.14 | 7.64 |
| 5 | CVE-2016-2346 | 6.8 | 2016-04-25 | Medium | N | 85 | 0.72 | 7.52 |
| 6 | CVE-2016-4521 | 10.0 | 2016-05-30 | Critical | N | 50 | 2.3 | 10 |
| 7 | CVE-2016-4051 | 6.8 | 2016-04-25 | Medium | Y | 85 | 0.14 | 6.14 |
| 8 | CVE-2015-7988 | 7.5 | 2016-06-25 | High | Y | 25 | 0.37 | 7.87 |
| 9 | CVE-2016-5020 | 9.0 | 2016-06-30 | High | N | 20 | 0.43 | 9.43 |
| 10 | CVE-2016-4440 | 7.2 | 2016-06-27 | High | Y | 23 | 0.27 | 7.47 |
| 11 | CVE-2016-5728 | 5.6 | 2016-06-27 | Medium | N | 23 | 1.2 | 6.8 |
| 12 | CVE-2016-3651 | 6.0 | 2016-06-30 | Medium | N | 20 | 0.74 | 6.74 |
| 13 | CVE-2016-1387 | 9.0 | 2016-05-05 | High | Y | 75 | 2.3 | 10 |
| 14 | CVE-2016-1343 | 6.4 | 2016-04-30 | Medium | Y | 80 | 1.5 | 7.9 |
| 15 | CVE-2016-0892 | 4.3 | 2016-05-03 | Medium | Y | 77 | 0.9 | 5.2 |
| 16 | CVE-2016-3092 | 7.8 | 2016-07-04 | High | Y | 16 | 1.09 | 8.89 |
| 17 | CVE-2016-4438 | 7.5 | 2016-07-04 | High | N | 16 | 1.05 | 8.55 |
| 18 | CVE-2015-7029 | 10.0 | 2016-07-02 | Critical | N | 18 | 0.42 | 10 |
| 19 | CVE-2016-1289 | 10.0 | 2016-07-02 | Critical | N | 18 | 1.71 | 10 |
| 20 | CVE-2016-1328 | 7.8 | 2016-07-03 | High | N | 17 | 0.84 | 8.64 |
| 21 | CVE-2016-1394 | 7.5 | 2016-07-02 | High | N | 18 | 0.45 | 7.95 |
| 22 | CVE-2016-1416 | 10.0 | 2016-07-02 | Critical | N | 18 | 0.35 | 10 |
| 23 | CVE-2016-1442 | 9.0 | 2016-07-07 | Critical | Y | 13 | 1.02 | 10 |
| 24 | CVE-2016-4512 | 7.5 | 2016-07-03 | High | N | 17 | 0.64 | 8.14 |
| 25 | CVE-2016-0230 | 7.2 | 2016-07-07 | High | N | 13 | 0.23 | 7.43 |

## 7.1 Observations

In above table SN 2,3 and 4 all vulnerabilities are having same severity level and maturity, as reported on the same date '2016-04-19' according to the US-CERT Cyber Security Bulletin [20]. All these are software vulnerability reported in

Red Hat Enterprise Linux 7. Red Hat releases patch for CVE-2015-8778 and CVE-2015-8779 [21], while patch is not available for CVE-2014-9761. After applying the proposed methodology, we observed that risk level of CVE-2014-9761 becomes 8.52 while risk level of CVE-2015-8778 and CVE-2015-8779 become 7.62 and 7.64 respectively, because of the availability of the patches. In the similar way vulnerability SN 5 "CVE-2016-2346" has severity score 6.8 released on 2016-04-25 and the qualitative severity level of the vulnerability is Medium. One another vulnerability SN 7 "CVE-2016-4051" also has the same CVSS score released on same date and having same qualitative severity level as CVE-2016-2346 vulnerability. It is reported in squid and it allows remote attackers to cause a denial of service or execute arbitrary code by seeding manager reports with crafted data.CVE-2016-4051 affects Linux systems Red Hat Enterprise Linux 6 (squid), Red Hat Enterprise Linux 6 (squid34) and Red Hat Enterprise Linux 7 (squid) on 2016-05-31 [22]. Rapid 7 released patch for this vulnerability, on 2016-06-14[23]. Even though both vulnerabilities have same severity level but patch is not available for CVE-2016-2346.After applying the proposed methodology, we observed that risk level of CVE-2016-2346 is 7.52 while risk level of CVE-2016-4051 is 6.14, because of the availability of the patch. After Qualitative evaluation, now severity level of CVE-2016-2346 is High while of CVE-2016-2346 is Medium. This evaluation shows that the proposed quantitative risk level evaluation of vulnerability will be more helpful in system security as it provides an effective way for risk level evaluation.

# 8. CONCLUSION

Controlling security risks is important for systems' safety as security attacks may lead to system failure. In order to control security risks the effective evaluation of risks level is essential. This paper presents the Enhanced Quantitative CVSS Risk Level Estimation Model which effectively determines the risk level of vulnerability. The proposed model computes the overall risk level of a system based on maturity and frequency estimates. The model uses attributes from the Base metrics to estimate frequency. From these attributes by using Base score equation of CVSS 3.0 severity of the vulnerability is calculated. Severity score is an important factor of measuring risk level of system. We are considering that severity of vulnerability affects the system but its proportion changes with time. To reflect change in risk level with time we converge the maturity of exploit with the severity of vulnerability.

The proposed framework introduced a new dimension for calculating frequency of the vulnerability with the assumption that the more frequent occurrences of vulnerability makes system riskier. The assumption behind frequency computation is that, a highly exploitable vulnerability is more likely to be misused by attackers and consequently should have a higher frequency. With this assumption, frequency of vulnerability is calculated with convergence of maturity of exploit. Finally, along with the frequency of vulnerability, severity and maturity of exploit the quantitative risk level is calculated which defines the security risk level of the system. The proposed Quantitative Risk Level evaluation model will enhance the system security by effective risk level measurement.

# 9. ACKNOWLEDGMENTS

The authors are highly thankful to Madhya Pradesh Council of Science and Technology, Bhopal for providing financial grant and support for this research project.

# 10. REFERENCES

[1] The Common Vulnerability Scoring System, Available: https://www.first.org/cvss

[2] National Vulnerability Database, Available: http://nvd.nist.gov

[3] A. Tripathi and U.K. Singh, "On prioritization of vulnerability categories based on CVSS scores", Proceedings of 6th International Conference on Computer Sciences and Convergence Information Technology, Korea, 2011, pp.692–697.

[4] A. Tripathi and U.K. Singh, "A proposal for common vulnerability classification scheme based on analysis of taxonomic features in vulnerability databases", International Journal of Computer Science and Information Security, Vol. 9, No. 6, 2011, pp.106–111.

[5] A. Tripathi and U.K. Singh, "Analyzing trends in vulnerability classes across CVSS metrics", International Journal of Computer Applications, Vol. 36, 2011, No. 3, pp.38–44.

[6] A. Tripathi and U.K. Singh, "Estimating risk level for vulnerability categories using CVSS", International Journal of Internet Technology and Secured Transactions", Vol. 4, No. 4, pp.272–289.

[7] C. Joshi and U. Singh, "Analysis of Vulnerability Scanners in Quest of Current Information Security Landscape" International Journal of Computer Application (IJCA, 0975 – 8887), Volume 145 No 2, July 2016, pp. 1-7.

[8] C. Joshi and U. Singh, "A Review on Taxonomies of Attacks and Vulnerability in Computer and Network System".International Journal of Advanced Research in Computer Science and Software Engineering (IJRCSSE) Volume 5, Issue 1, January 2015, pp 742-747.

[9] C. Joshi C. and U. Singh, "ADMIT- A Five Dimensional Approach towards Standardization of Network and Computer Attack Taxonomies". International Journal of Computer Application (IJCA, 0975 – 8887), Volume 100, Issue 5, August 2014, pp 30-36.

[10] R. E. Sawilla and X.Ou,, "Identifying critical attack assets in dependency attack graphs". In: ESORICS '08: Proceedings of the 13th European Symposium on Research in Computer Security, Malaga, Spain, Springer-Verlag, 2008, pp. 18–34.

[11] W.U. Bin and A. J. WANG, "EVMAT: An OVAL and NVD Based Enterprise Vulnerability Modeling and Assessment Tool", In Proceedings of ACMSE, Kennesaw, GA, USA, March 24-25, 2011, pp.115-120.

[12] "Risk Assessment and Mapping Guidelines for Disaster Management", COMMISSION STAFF WORKING PAPER, Brussels, 2010.

[13] CVE - Common Vulnerabilities and Exposures (CVE), Available: https://cve.mitre.org/

[14] T. Hamid, C Maple, P. Sant., "Methodologies to Develop Quantitative Risk Evaluation Metrics", International Journal of Computer Applications, Vol. 48 No.14, June 2012, pp.17-24.

[15] CVSS v3.0 specification document, Available: https://www.first.org/cvss/specification-document

[16] P. Mell, K. Scarfone, and S. Romanosky, "CVSS: A complete Guide to the Common Vulnerability Scoring System Version 2.0", Forum of Incident Response and Security Teams (FIRST), 2007.

[17] A. Arora., R. Krishnan,R.Telang, Y. Yang, "An Empirical Analysis of Software Vendors' Patching Behavior: Impact of Vulnerability Disclosure", ICIS 2006 Proceedings, 2006, Paper 22.

[18] M. Ahmed, E. Al-Shaer and L. Khan, "A Novel Quantitative Approach for Measuring Network Security", INFOCOM 2008, The 27th Conference on Computer Communications, IEEE, 13-18 April 2008.

[19] Common Vulnerability Scoring System Version 3, Available: Calculatorhttps://nvd.nist.gov/CVSS/v3-calculator.

[20] Red Hat Customer Portal, Available: https://access.redhat.com/security/cve/cve-2016-4051.

[21] CVE-2016-4051: SECURITY PATCH FOR SQUID (ALAS-2016-713), Available: https://www.rapid7.com/db/vulnerabilities/amazon_linux-cve-2016-4051.

[22] Red Hat Customer Portalhttps://access.redhat.com/security/cve/cve-2016-4051.

[23] CVE-2016-4051: SecurityPatchforSquid (ALAS-2016-713)https://www.rapid7.com/db/vulnerabilities/amazon_linux-cve-2016-4051.