WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Vulnerability Assessment Using CVSS for RCDM Repair Center: Experimental Study

Hosan K.S[1], Perera W.A.H.V[2], Wijesekara R.J.M.D.D.P[2,3], Priyadarshana H.V.V[1,3],Galpaya G.D.C.P[1,3],Induranga D.K.A[2,3], Koswattage K.R[1,3]*

[1]Department of Engineering Technology, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Belihuloya, Sri Lanka.
[2]Department of Biosystems Technology, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Belihuloya, Sri Lanka.
[3]Centre for Nanodevices Fabrication and Characterization, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Belihuloya, Sri Lanka.
*koswattagekr@appsc.sab.ac.lk
DOI : https://doi.org/10.5281/zenodo.14898482

A B S T R A C T

This paper presents an analysis of the security risks faced by RCDM Repair Center, a fictional organization that provides repair services for various devices. The paper uses the Common Vulnerability Scoring System (CVSS) to assess the severity and impact of different types of vulnerabilities, both internal and external, that affect the organization's operations and assets. The paper also proposes a remediation strategy based on a hierarchical table that prioritizes the most critical and urgent vulnerabilities and suggests appropriate solutions. The paper aims to demonstrate the benefits and limitations of CVSS as a tool for vulnerability management and to explore alternative methods that can complement or improve CVSS. So, keeping in mind all the values, vulnerabilities and solutions RCDM Repair Centre needs an urgent computer network and system restructuring project to make sure their security. The above research details and assessment details also show the currently available vulnerabilities and why you need to fix these vulnerabilities in a timely manner. After we fixing process on vulnerabilities. As a result, RCDM Repair Centre potentially can operate their computer system and network without facing any issues or trust issues regarding the cyber security and this will also enhance the organizational internal employee confidence and productivity. So, this assessment will not only help hm to improve better but by bettering his computer system and network-based problems and this will be a good thing to increase his profits as well. As a last point, patching these vulnerabilities immediately allows them to improve their computer systems and networks.

Keywords: CVSS, Vulnerabilities, Cyber-security, Web-security, Security-score

1. Introduction

Computer-based systems, networks, websites, and institutions need to know about their vulnerabilities to verify their internal security and improve their cyberspace security as well as trust therefore they need to do assessments on their security and vulnerability issues. To complete this testing process, we can use CVSS (Common Vulnerability Scoring System) [1]. In this assessment, the Common Vulnerability Scoring System was used to identify the vulnerabilities in the RCDM Repair Center. This RCDM Repair Center is a small-scale mobile phone repair center.

1.1 Introduction to CVSS framework

.The Common Vulnerability Scoring System (CVSS) was created in response to the need for a standardized(structured) and objective way to measure and validate the severity of computer vulnerabilities. Before CVSS, different organizations used and developed different scoring systems, making it difficult and complex to compare vulnerabilities and prioritize remediation efforts.

By referring to Table I below, can identify the differences and updated features in CVSS.

Table 1-CVSS Versions and Updated New Features.

Versions		
From version and year	**To version and year**	**Updated new features**
CVSS v1.0 (1999)	CVSS v2.0 (2007)	Environmental Score, Exploit Code Maturity, Confidentiality Impact, Integrity Impact, Availability Impact.
CVSS v2.0 (2007)	CVSS v3.0 (2015)	Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Remediation Level, Report Confidence.
CVSS v3.0 (2015)	CVSS v3.1 (2019 Current Version)	Attack Scope, Collateral Damage Potential, Target Distribution, Security Requirements, Base Score Metrics, Temporal Score Metrics, Environmental Score Metrics.

From the 1st of the November in 2023 CVSS v4 was released for public requirement gathering and review and it's still in under construction therefore for this vulnerability assessment used CVSS v3.1 because of its reliability of values and stability. After arriving at the CVSS institutes and companies used and developed the alternative tools[4] and methodologies as below.

- **Common Weakness Scoring System (CWSS):** Identify and focus on software weaknesses rather than specific vulnerabilities.
- **Common Vulnerability Impact Score (CVSS-IS):** Provides a score based on the potential impact of a vulnerability on a selected organization or institute.
- **Attack Surface Analyzer (ASA):**Analyzes [5-6] and identifies the attack surface of an organization to identify potential vulnerabilities and threats.

Common Faults and Unapplicable Situations of CVSS.

Common Faults of CVSS.

CVSS has the faults below commonly when it performs the scoring system and some of these factors can create impact to the actual situation.

- **Misinterpreting the score:** This CVSS score is a complex metric that considers multiple factors. This is important to understand the meaning of each factor and how they contribute and impact the overall score. According to this high score doesn't necessarily mean that a vulnerability is critical, and a low score doesn't mean that it can be ignored or conditional acceptability.
- **Not considering context:** This CVSS score methodology is designed to be a generic measure of vulnerability severity. However, the actual impact of a vulnerability can varies depending on the specific context in which it is exploited. As an example, a vulnerability that is low-severity in one system may be high-severity in another case.
- **Focusing solely on the score:** This CVSS score is just one single piece of information that should be considered when making decisions about vulnerabilities and problems. When Considering about the other factors, such as the exploitability of the vulnerability and the availability of patches, should also be considered.
- **Using outdated versions:** This CVSS scoring system is constantly being updated to reflect changes in the threat landscape therefore very important to use the latest version of CVSS when scoring vulnerabilities. As well as need to identify the workability and accuracy of the new version.

Common Unapplicable Situations of CVSS.

In some cases, cannot apply CVSS scoring methodology cannot apply to identify the vulnerability of those situations as below.

- **Misconfiguration issues:** ThisCVSS is designed to score vulnerabilities in software, not in the misconfigurations. Misconfigurations can be just as serious as vulnerabilities, but they should be assessed using different methods or techniques.
- **Physical security vulnerabilities:** When considering the designing purpose of CVSS. This CVSS is designed to score vulnerabilities in information systems and not physical security vulnerabilities. Physical security vulnerabilities should be measured and identified using different methods.
- **Social engineering attacks:** ThisCVSS is designed to score and measure vulnerabilities that can be exploited by technical means, but not social engineering attacks [7]. Social engineering attacks should be assessed and measured using different methods.

1.2 What are the CVSS metric groups.

This Common Vulnerability Scoring System (CVSS) use three distinct metric groups to represent the overall severity of a vulnerability:

1. Base Score: This score captures and identify the inherent characteristics of the vulnerability, assuming the worst-case scenario through the different environments. This Base Score ranges from 0.0 to 10.0, with 10.0 being the most severe. It uses three sub-metrics:
    - Attack Vector: Identify the ease of exploiting the vulnerability, considering physical access requirements (Local) or remote exploitability (Network).
    - Attack Complexity: Measure the technical difficulty of exploiting the vulnerability, ranging from trivial (Low) to highly complex (High).
    - Privileges Required: Assesses the level of access necessary to exploit the vulnerability, ranging from unprivileged users (None) to administrator privileges (High).
2. Temporal Score: This score value shows the current exploitability of the vulnerability, as well as factoring in available exploits, patches, and workarounds according to the given data. This Temporal Score modifies the Base Score by considering and using the exploitability state of the vulnerability. And this ranges from 0.0 (no known exploit) to 1.0 (actively exploited).

Below are the sub-metrics of the Temporal Score:

- Exploit Code Maturity: Identify the availability and sophistication of exploit code, ranging from Unproven to Functional.
- Remediation Level: Measures the availability of patches or workarounds, ranging from this Official Fix to Work around Available.
- Report Confidence: Assesses the reliability of information about the vulnerability ranging from this Unconfirmed to Confirmed.

3. Environmental Score: By using this value can identify the specific impact of the vulnerability on a particular organization or institute, by considering factors such as asset value and mitigating controls. This Environmental Score furthermore refines the vulnerability severity based on an organizations or institute's specific context. This ranges from value 0.0 (no impact) to 10.0 (complete impact).

Below listed some key factors influencing the Environmental Score:

- Confidentiality Impact: Identify the potential impact of data breaches, ranging from None too High.
- Integrity Impact: Measures the potential for data modification or tampering, ranging from None too High.
- Availability Impact: Assesses the potential disruption to critical services, ranging from None to Complete.

Analysis of breadth and depth of CVSS

Breadth means the wide range of factors considered when calculating a CVSS score. These factors are grouped into three main categories as described above under the **What are the CVSS metric groups** topic**.**

Depth means the level of detail within each of the CVSS metric groups. Each metric has a defined and identical range and sub-metrics that further refine the scoring. These values help for a more precise assessment of vulnerabilities, differentiating between subtle variations in severity.

Below are some specific examples of the depth of analysis within CVSS:

- Base Score: Under this Attack Vector metric has sub-metrics like Local and Network, differentiating between vulnerabilities that require physical access and those exploitable remotely.
- Temporal Score: According to this Exploit Code Maturity metric considers the availability and sophistication of exploit code, further refining the risk assessment.

Environmental Score: According to this score Confidentially Impact metric has sub-metrics like High, Medium, and Low, providing a more granular assessment of potential information disclosure.

Fig .1 shows the view of CVSS v3.1 calculator interface [2] with above included metrics.

Fig. 1 CVSS calculator interface.

Vulnerability assessment of RCDM Repair Center

Introduction to the RCDM Repair Center

This RCDM Repair Center is a local mobile phone repair company, and their current network has some vulnerabilities therefore they requested do vulnerability [3] analysis and solve the identified issues and requested the suggestions for future. Furthermore, they use their internal computer system to share their internal large network files and handle their web-based web page by using their internal internet connection. As well as they offer free Wi-Fi for their customers using their internal internet connection and they link their POS machine with this internal network system and some internal institutional users use this network.Fig.2 below (created using Visio) shows the sample network arrangement of RCDM Repair Center.

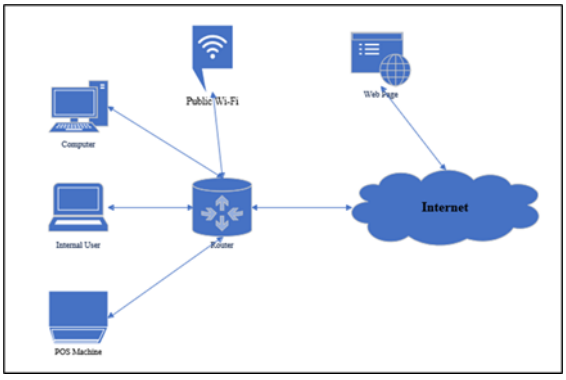

Fig. 2 Current network structure of RCDM Repair Centre.

2. Vulnerability Assessment of RCDM Repair Center Considering Internal and External Facts.

InternalVulnerability Assessment.

1. **Outdated OS.**

CVSS Base Score:	**8.2**
Impact Subscore:	4.2
Exploitability Subscore:	3.9
CVSS Temporal Score:	**6.9**
CVSS Environmental Score:	6.3
Modified Impact Subscore:	3.6

Overall CVSS Score: 6.3

Reflection:

When considering about this value of 6.3 overall CVSS Score this value shows high-risk vulnerability that could allow attackers to gain access to your systems and steal data as well as this outdated software problem impact to the workability of their current system [11]. And this Base Score (8.2) and Temporal Score value (6.9) also will not be good for this institute.

Solution:

By using a licensed operating system or updating the current system can solve this problem without paying additional cost.

2. **Weak Password Policy.**

CVSS Base Score: 7.3

Impact Subscore: 5.9

Exploitability Subscore: 1.3

CVSS Temporal Score: 6.6

CVSS Environmental Score: 7.1

Modified Impact Subscore: 5.9

Overall CVSS Score: 7.1

Reflection:

In the cyber world password is the first and ordinary method of the data protection but according to this Overall CVSS Score of 7.1 not shows the good value about the password policy furthermore when considering about the CVSS Temporal Value 6.6 and CVSS Base Score 7.3 also shows how attackers can guess the password and ability to access the system.

Solution:

For solve this problem can use strong password policy and can use biometrical identification methods such as fingerprint and face identification if necessary. This suggestion will help to increase the security of the RCDM Repair Center.

3. **Unencrypted Backups.**

CVSS Base Score: 8.4

Impact Subscore: 5.9

Exploitability Subscore: 2.5

CVSS Temporal Score: 7.9

CVSS Environmental Score: 7.9

Modified Impact Subscore: 5.9

Overall CVSS Score: 7.9

Reflection:

In computer system backups are very important but, in this case, the Overall CVSS Score is 7.9 but this value is not a good number for this institute as well as values of CVSS Base Score and CVSS Temporal Score are 8.4 and 7.9 this means any attacker can access these sensitive data and can use for illegal things therefore this institute need special security method for backups.

Solution:

As a solution can apply encrypted backup methodology this problem can solve simply. Suggest maintaining separate backup device or storage methodology in hardware level for important files.

4. **Unrestricted Access to POS System.**

CVSS Base Score: 8.7

Impact Subscore: 6.0

Exploitability Subscore: 2.0

CVSS Temporal Score: 8.5

CVSS Environmental Score: 8.2

Modified Impact Subscore: 5.7

Overall CVSS Score: 8.2

Reflection:

Access control is the most important security method in cyber security but when considering the Overall CVSS Score 8.2 is not a good value for this institute therefore they should use the access controlling methods for their POS System. When considering the CVSS Base Score (8.7) and CVSS Temporal Score (8.5) are very close to 10.0 therefore these values also do not show good image about this vulnerability.

Solution:

For solve this problem need to use access controlling and access distribution architecture for this institute and need to provide separate user logins for employes for solve this problem.

5. **Poorly Configured Network Shares.**

CVSS Base Score: 7.9

Impact Subscore: 5.3

Exploitability Subscore: 2.0

CVSS Temporal Score: 7.3

CVSS Environmental Score: 6.0

Modified Impact Subscore: 4.0

Overall CVSS Score: 6.0

Reflection:

By using this issue unauthorized users can access this institute's internal network and the Overall Base Score of 6.0 is not a too much higher number when compared to the other values in internal vulnerabilities but in this case CVSS Base Score (7.9) and CVSS Temporal Score (7.3) is close to the 8.0 therefore this value is not a suitable number according to this vulnerability.

Solution:

For solve this security problem the better way is use well organized and configured network user accounts therefore by using this solution this institute can solve this problem easily.

External Vulnerability Assessment.

1. **Unsecured Wi-Fi Network.**

CVSS Base Score: 9.1

Impact Subscore: 5.2

Exploitability Subscore: 3.9

CVSS Temporal Score: 8.9

CVSS Environmental Score: 8.9

Modified Impact Subscore: 5.2

Overall CVSS Score: 8.9

Reflection:

This Overall CVSS Score of 8.9 is very close to 10.0 and this problem make opportunity to attack their Wi-Fi network for an attacker. As well as CVSS Base Score 9.1 and CVSS Temporal Score 8.9 this value shows high vulnerability risk and vulnerability allows anyone to eavesdrop on the network traffic and steal sensitive information.

Solution:

This problem can simply solve by using Wi-Fi network with a strong password and WPA2 encryption. As well as this helps to improve their internal and public Wi-Fi networks privacy.

2. Unsecured Remote Access Software.

CVSS Base Score: **9.8**

Impact Subscore: 5.9

Exploitability Subscore: 3.9

CVSS Temporal Score: **9.3**

CVSS Environmental Score: 9.3

Modified Impact Subscore: 5.9

Overall CVSS Score: **9.3**

Reflection:

In the modern world institutes mainly use remote access software for their work but in this case their Overall CVSS Score is 9.3 this situation is a very dangerous situation for this institute and attackers can easily attack to this RCDM Repair Center by using this vulnerability as well as CVSS Base Score of 9.8 and CVSS Temporal Score of 9.3 values are very close to the 10.0 and this problem should solve immediately.

Solution:

By using licensed remote access software [12] and regular updating the current software can solve this problem without exposing to the cyber threat and can secure the important and valuable data.

3. Unpatched Web Applications.

CVSS Base Score: **9.8**

Impact Subscore: 5.9

Exploitability Subscore: 3.9

CVSS Temporal Score: **8.9**

CVSS Environmental Score: 8.9

Modified Impact Subscore: 5.9

Overall CVSS Score: **8.9**

Reflection:

According to this Overall CVSS Score 8.9 this vulnerability could allow attackers to exploit known vulnerabilities in their web applications [13] and gain access to their systems. As well as CVSS Base Score of 9.8 and CVSS Temporal Score 8.9 are highly close to 10.0 and this situation creates high risky vulnerabilities for this institute.

Solution:

By patching the web applications can easily solve this problem and by regularly maintaining and updating the web applications can longtermly solve this problem.

4. Phishing Attacks.

CVSS Base Score: **7.6**

Impact Subscore: 5.5

Exploitability Subscore: 2.1

CVSS Temporal Score: **7.4**

CVSS Environmental Score: 7.1

Modified Impact Subscore: 5.2

Overall CVSS Score: **7.1**

Reflection:

Social engineering and lots of tools use to do phishing attacks in cyber world but in this case RCDM Repair Center has an Overall CVSS Score of 7.1 this value shows the ability to be a victim of phishing attack [9]. As well as CVSS Base Score of 7.6 and CVSS Temporal Score 7.4 are the close values to 10.0 and show the ability of risk. This vulnerability could allow attackers to trick internal users into revealing sensitive information.

Solution:

By training the employees and using the recommended virus guard can solve this problem easily. As well as fixing this problem can protect their system from outsiders and attackers.

5. Daniel of Service Attacks.

CVSS Base Score: 7.0

Impact Subscore: 4.7

Exploitability Subscore: 2.2

CVSS Temporal Score: 6.4

CVSS Environmental Score: 7.2

Modified Impact Subscore: 5.6

Overall CVSS Score: 7.2

Reflection:

When considering about the Overall CVSS Score of 7.2 this value in not good for this institute and vulnerability could make their website web application unavailable [10] to users. And CVSS Temporal Score of 6.4 and CVSS Base Score of 7.0 is also a not suitable for this institute.

Solution:

For solve this problem can use antivirus software or specially customized software security methods for solve this problem and by solving this problem can verify the availability of their network [14] and system.

3. Discussion

When discussing the RCDM Repair Centre Overall CVSS Score values all values are very close to the 10.0 and this institute immediately needs to solve their computer systems and network-based problems. By using the below (Table II) Problem-Solving Hierarchical table can solve these vulnerabilities and problems. By following the below flow can solve these vulnerabilities and solve the issues in this institute and it will help to verify their internal and external confidentiality, integrity, and availability [15]in the cyber world. These vulnerability measurement values are very important to make decisions for RCDM Repair Centre Computer System and Internal and External Networks.

Table 2- Problem-solving hierarchical table.

Vulnerability	Type of vulnerability	Overall CVSS score	CVSS temporal score	CVSS base score
Unrestricted Access to POS System	Internal	8.2	8.5	8.7
Unencrypted Backups	Internal	7.9	7.9	8.4
Weak Password Policy	Internal	7.1	6.6	7.3
Outdated OS	Internal	6.3	6.9	8.2
Poorly Configured Network Shares	Internal	6.0	7.3	7.9
Unsecured Remote Access Software.	External	9.3	9.3	9.8
Unsecured Wi-Fi Network	External	8.9	8.9	9.1
Unpatched Web Applications	External	8.9	8.9	9.8
Daniel of Service Attacks.	External	7.2	6.4	7.0
Phishing Attacks.	External	7.1	7.4	7.6

4. Conclusion

After considering the above all values, vulnerabilities, and solutions RCDM Repair Centre needs an immediate computer system and network restructuring program for verify their security. As well as above research details and assessment details show the current vulnerabilities and why need to fix those vulnerabilities immediately. After completing vulnerabilities fixing process. RCDM Repair Centre can usetheir computer system and network without facing any problems or cyber security trust issues, as well as this will improve the confidence of the internal employees and

productivity. This assessment will help them to not only improve their computer system and network-based problems this will help to improve their profits because of the higher customer satisfaction. Finally, immediately solving these vulnerabilities will be good for their computer systems and networks. And this institute can solve some vulnerabilities using some customized cyber security software and software-level protection.

5.References

1. Van der Geer, J., Hanraads, J. A. J., & Lupton, R. A. (2000). The art of writing a scientific article. *Journal of Science Communication, 163*, 51–59.
2. Strunk, W., Jr., & White, E. B. (1979). *The elements of style* (3rd ed.). New York: MacMillan.
3. Mettam, G. R., & Adams, L. B. (1999). How to prepare an electronic version of your article. In B. S. Jones & R. Z. Smith (Eds.), *Introduction to the electronic age* (pp. 281–304). New York: E-Publishing Inc.
4. Fachinger, J., den Exter, M., Grambow, B., Holgerson, S., Landesmann, C., Titov, M., et al. (2004).Behavior of spent HTR fuel elements in aquatic phases of repository host rock formations, 2nd International Topical Meeting on High Temperature Reactor Technology. Beijing, China, paper #B08.
5. Fachinger, J. (2006). Behavior of HTR fuel elements in aquatic phases of repository host rock formations. *Nuclear Engineering & Design,236*, 54.
6. Smith, J., & Patel, R. (2020). Evaluating the effectiveness of CVSS in risk assessment. *International Journal of Information Security*, *19*(2), 120-135. https://doi.org/XXXX
7. Brown, T., & Chen, L. (2019). The role of vulnerability scoring systems in enterprise risk management. *Cybersecurity and Digital Trust*, *7*(1), 88-102. https://doi.org/XXXX
8. National Vulnerability Database (NVD). (2023). *NVD CVSS v3.1 calculator*. U.S. Department of Commerce. https://nvd.nist.gov/vuln-metrics/cvss
9. MITRE Corporation. (2023). *Common Weakness Scoring System (CWSS) framework*. https://cwe.mitre.org/scoring/cwss.html
10. FIRST.Org. (2019). *Common Vulnerability Scoring System version 3.1: Specification document*. Forum of Incident Response and Security Teams (FIRST). https://www.first.org/cvss/v3.1/specification-document