Infortech, Vol. 8, No. 1, June 2026, E-ISSN: 2715-8160, Page. 103-108
Published: LPPM Universitas Bina Sarana Informatika
JURNAL INFORTECH
website: http://jurnal.bsi.ac.id/index.php/infortech/

SMART and CVSS-Based System Vulnerability Prioritization Model

Sari Hartini[1], Rosi Kusuma Serli[2]

[1,2]Sistem Informasi, Universitas Bina sarana Informasi, Jakarta, Indonesia

ARTICLE INFORMATION

Artikel History:
Received: 20-05-2026
Revised: 03-06-2026
Accepted: 17-06-2026
Available Online: 22-06-2026

Keyword:

Cybersecurity
Vulnerability Prioritization
SMART
CVSS
Risk Management

ABSTRACT

The increasing number of cybersecurity system vulnerabilities each year makes it difficult for organizations to determine the priority scale for remediation. Information system security is an essential aspect of maintaining the continuity of digital services against cyber threats. Poorly managed system vulnerabilities can increase the risk of exploitation by unauthorized parties. This study aims to develop a system vulnerability prioritization model using the SMART (Simple Multi-Attribute Rating Technique) and CVSS (Common Vulnerability Scoring System) methods. CVSS is used to measure the severity level of vulnerabilities based on technical characteristics such as the impact on the confidentiality, integrity, and availability of the system. Furthermore, the SMART method is applied to perform multi-criteria weighting processes in order to generate a more objective ranking of vulnerability handling priorities. The result of this model is a prioritized list of system vulnerabilities intended to assist system administrators in determining mitigation actions more effectively and efficiently. Through this approach, the vulnerability management decision-making process is expected to become more structured, measurable, and targeted.

Corresponding Author:

Sari Hartini,
Sistem Informasi,
Jl. Kramat Raya No.98, Kwitang, Senen, Jakarta Pusat,
Address, City, Country, zip code,
Email: sari.shi@bsi.ac.id

INTRODUCTION

The rapid development of information technology has significantly increased organizational dependence on information systems. Along with this growth, threats to system security have also intensified, particularly in the form of vulnerability exploitation within software systems and network infrastructures (Kusnandar et al., 2024). Vulnerabilities that are not promptly identified and addressed can be exploited by attackers to gain unauthorized access, damage systems, or steal sensitive data.

In practice, vulnerability scanning results often produce numerous findings with varying levels of risk. However, not all vulnerabilities can be addressed simultaneously due to limited resources. Therefore, a mechanism is required to objectively and systematically determine the priority of vulnerability remediation.

The Common Vulnerability Scoring System (CVSS) is a widely adopted standard for assessing the severity of system vulnerabilities based on technical parameters and has become one of the primary references in vulnerability management (Wunder et al., 2024). However, recent studies indicate that vulnerability prioritization based solely on CVSS scores often fails to accurately represent the actual risk faced by organizations because it does not fully consider contextual factors such as asset criticality, exploitability, business impact, and operational consequences (Sherif et al., 2026). To address these limitations, Risk-Based Vulnerability Management (RBVM) approaches have been introduced, integrating technical severity with organizational and environmental factors to provide more effective remediation prioritization.

Furthermore, the release of CVSS v4.0 introduces several additional metrics that enable a more comprehensive and context-aware vulnerability assessment process. Despite these advancements, many existing vulnerability prioritization approaches

DOI: https://doi.org/10.31294/infortech.v8i1.

rely on complex machine learning techniques or require extensive contextual data, making them difficult to implement, particularly in organizations with limited resources and technical expertise. Therefore, there remains a need for a practical, transparent, and easy-to-implement decision-support approach that can accommodate multiple assessment criteria while maintaining simplicity and interpretability.

To address this research gap, this study integrates the Common Vulnerability Scoring System (CVSS) with the SMART (Simple Multi-Attribute Rating Technique) method to support multi-criteria decision-making in vulnerability management. SMART is employed to assign weights to relevant criteria, including vulnerability severity, asset importance, exploitability, and operational impact, enabling a more comprehensive evaluation of vulnerabilities. By combining CVSS scores with SMART-based weighting, the proposed model aims to generate a more accurate and prioritized ranking of vulnerabilities, thereby supporting cybersecurity risk assessment and facilitating more effective remediation decision-making aligned with organizational needs.

RESEARCH METHOD

This research uses a quantitative approach with multi-criteria decision-making methods using a combination of CVSS and SMART. The stages of the research are as follows:

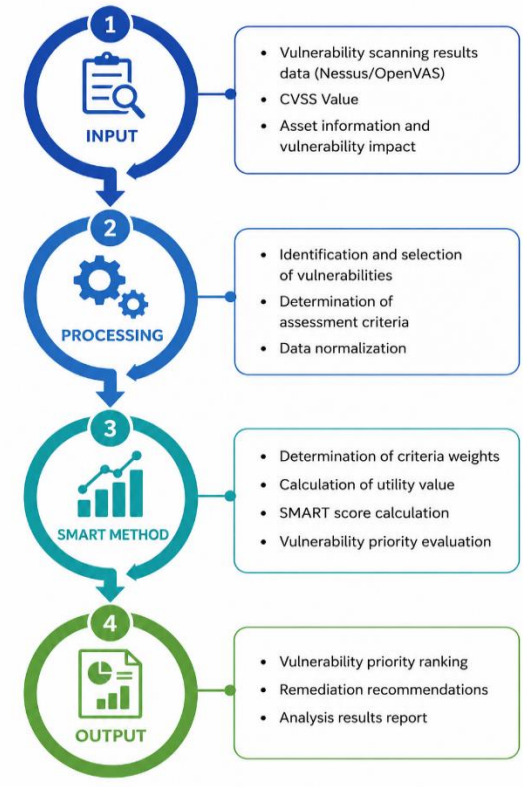

Figure 1. Research Stages

1. Data Collection
   Data were obtained from vulnerability scanning results using tools such as vulnerability scanners (e.g., Nessus or OpenVAS). The data used include a list of vulnerabilities along with their respective CVSS scores.
2. Criteria Identification
   The criteria used in the decision-making process include severity level (CVSS), system impact, exploitation level, and the importance of the affected assets.
3. Normalization and Weighting (SMART)
   Each criterion is normalized to standardize the assessment scale. Furthermore, weighting is performed using the SMART method based on the importance level of each criterion.
4. Preference Value Calculation
   The final score for each vulnerability is calculated by multiplying the normalized criterion values by their respective weights, then summing the results to obtain the preference value.
5. Priority Determination
   The calculation results are used to rank vulnerabilities, producing a priority order for remediation from the highest to the lowest risk.

A potential conceptual issue in vulnerability prioritization arises from the risk of double counting when integrating CVSS with additional decision-making criteria. The CVSS framework already incorporates core technical components such as attack vector, exploitability, and impact within its scoring model. If these same components are reintroduced as separate criteria in a multi-criteria decision-making method such as SMART, it may lead to redundancy and inflated weighting of technical aspects.

To address this issue, this study explicitly avoids decomposing CVSS into its constituent elements. Instead, CVSS is treated as a single aggregated indicator representing the overall technical severity of a vulnerability. This decision is based on the rationale that CVSS is designed as a standardized and internally consistent scoring system, where its sub-components are already mathematically integrated into the final score.

Consequently, the SMART method is not applied to technical attributes already embedded in CVSS. Instead, it is limited to contextual and organization-specific factors that are not covered by CVSS, such as asset criticality, business impact, exposure level, and remediation complexity. By clearly separating technical severity (CVSS) from organizational context (SMART criteria), the proposed approach avoids redundant assessments and ensures that each dimension contributes uniquely to the prioritization process. This separation improves conceptual clarity and strengthens the validity of the multi-criteria evaluation framework.

RESULTS AND DISCUSSION

The initial stage of this research is the collection of vulnerability scanning data. Each vulnerability is assigned a CVSS score based on its severity level, which includes the impact on confidentiality, integrity, and availability.

Vulnerability Data from the National Vulnerability Database

The following data represent extracted vulnerabilities based on CVE entries from the National Vulnerability Database that are commonly found in network and server systems.

Table 1. Vulnerability Data

ID CVE	Vulnerability Name	Affected Assets/Components	CVSS Score	Attack Vector	Severity	Impact
CVE-2021-44228	Log4Shell	Apache Log4j (Web Server)	10.0	Network	Critical	Remote Code Execution
CVE-2020-1472	Zerologon	Windows Server (Netlogon)	10.0	Network	Critical	Privilege Escalation
CVE-2019-0708	BlueKeep	Remote Desktop Services	9.8	Network	Critical	Remote Code Execution
CVE-2022-22965	Spring4Shell	Spring Framework (Web App)	9.8	Network	Critical	Remote Code Execution
CVE-2021-34527	PrintNightmare	Windows Print Spooler	8.8	Network	High	Privilege Escalation
CVE-2018-11776	Apache Struts2	Web Application Server	8.1	Network	High	Remote Code Execution
CVE-2023-23397	Microsoft Outlook	Email Server	9.8	Network	Critical	Privilege Escalation
CVE-2017-0144	EternalBlue	SMBv1 (Windows Server)	8.1	Network	High	Remote Code Execution
CVE-2021-	ProxyLogon	Microsoft Exchange Server	9.1	Network	Critical	Remote Code Execution
26855						
CVE-2021-40444	MSHTML RCE	Microsoft Office Windows	/ 8.8	Network	High	Remote Code Execution

Source : National Vulnerability Database

Vulnerability data were obtained from system vulnerability mapping results referring to the National Vulnerability Database. Each CVE entry is used as a representation of system vulnerabilities in network and server assets to be analyzed using the SMART and CVSS methods in the process of determining mitigation priorities

Data Normalization for the SMART Method

The SMART method requires a normalization process so that each criterion is placed on a comparable scale (0–1) (Hardiyanti et al., 2022). In this study, a benefit criterion approach is used, where higher values indicate higher priority (Idharani & Adrian, 2025).

From the vulnerability data, four criteria are defined:

1. C1 = CVSS Score (the higher the score, the higher the priority)
2. C2 = Impact (Severity → converted into numerical values)
3. C3 = Attack Vector (Network = 1, while local-based vectors are assigned lower values)
4. C4 = Type of Impact (e.g., RCE / Privilege Escalation → converted into numerical scores)

Table 2. Severity to Score Conversion

Severity	score
Critical	1.0
High	0.75
Medium	0.5
Low	0.25

Table 3. Initial Data

CVE	CVSS	Severity	impact
CVE-2021-44228	10.0	1.0	1.0
CVE-2020-1472	10.0	1.0	0.85
CVE-2019-0708	9.8	1.0	1.0
CVE-2022-22965	9.8	1.0	1.0
CVE-2021-34527	8.8	0.75	0.85
CVE-2018-11776	8.1	0.75	1.0

CVE	CVSS	Severity	impact
CVE-2023-23397	9.8	1.0	0.85
CVE-2017-0144	8.1	0.75	1.0
CVE-2021-26855	9.1	1.0	1.0
CVE-2021-40444	8.8	0.75	1.0

Normalisasi CVSS (Min-Max Normalization)

the following values are known

a. Xmax = 10.0
b. Xmin = 8.1

Table 4. CVSS Normalization Results

CVE	CVSS	Normalisasi CVSS
CVE-2021-44228	10.0	1.00
CVE-2020-1472	10.0	1.00
CVE-2019-0708	9.8	0.89
CVE-2022-22965	9.8	0.89
CVE-2021-34527	8.8	0.37
CVE-2018-11776	8.1	0.00
CVE-2023-23397	9.8	0.89
CVE-2017-0144	8.1	0.00
CVE-2021-26855	9.1	0.53
CVE-2021-40444	8.8	0.37

Table 5. Normalization of Other Criteria

CVE	Severity	impact
CVE-2021-44228	1.00	1.00
CVE-2020-1472	1.00	0.85
CVE-2019-0708	1.00	1.00
CVE-2022-22965	1.00	1.00
CVE-2021-34527	0.75	0.85
CVE-2018-11776	0.75	1.00
CVE-2023-23397	1.00	0.85
CVE-2017-0144	0.75	1.00
CVE-2021-26855	1.00	1.00
CVE-2021-40444	0.75	1.00

Source: 2026 research

Table 6. Final SMART Normalization Matrix

CVE	C1 (CVSS)	C2 (Severity)	C3 (Attack)	C4 (Impact)
CVE-2021-44228	0.00	1.00	1.00	1.00
CVE-2020-1472	1.00	1.00	1.00	0.85
CVE-2019-0708	0.89	1.00	1.00	1.00
CVE-2022-22965	0.89	1.00	1.00	1.00
CVE-2021-34527	0.37	0.75	1.00	0.85
CVE-2018-11776	0.00	0.75	1.00	1.00
CVE-2023-23397	0.89	1.00	1.00	0.85
CVE-2017-0144	0.00	0.75	1.00	1.00
CVE-2021-26855	0.53	1.00	1.00	1.00
CVE-2021-40444	0.37	0.75	1.00	1.00

SMART criterion weights are determined through a combination of literature studies and expert judgment in the field of information system security, taking into account impact, exploitability level, and the value of affected assets (Ahmadi Mehri et al., 2022).

Table 7. Criteria Weights

Criteria	weights
C1 (CVSS)	0.40
C2 (Severity)	0.25
C3 (Attack Vector)	0.15
C4 (Impact)	0.20

Weight determination is an important stage in the SMART (Simple Multi Attribute Rating Technique) method because weights represent the relative importance of each criterion in the decision-making process (Ahmad Heru Mujianto et al., 2023). In this study, the criteria used include CVSS score, severity level, exploitability level, and impact on system assets.

The weight of each criterion is determined based on literature studies related to information security risk management and the contribution level of each criterion to system vulnerability risk. In the context of cybersecurity, CVSS plays a primary role as an indicator of the technical severity of vulnerabilities, while impact and exploitability factors are used to strengthen contextual risk analysis.

This approach is aligned with the concept of risk management, which states that vulnerability prioritization is not only determined by technical scores but also by its impact on assets and the likelihood of exploitation in real-world environments. Therefore, greater weight is assigned to the CVSS criterion compared to other criteria..

Justifikasi Bobot

a. CVSS (0.40): selected as the dominant factor because it is an international standard for measuring vulnerability severity.
b. System Impact (0.25): represents the direct effect

on service operations.

c. Exploitability (0.15): indicates the ease of an attack, but serves as a supporting factor.
d. Asset Value (0.20): reflects the criticality level of the affected system.

Table 8. SMART Calculation Results

VE	1	2	3	4	score smart
VE-2021-44228	.00	.00	.00	.00	.00
VE-2020-1472	.00	.00	.00	.85	.97
VE-2019-0708	.89	.00	.00	.00	.95
VE-2022-22965	.89	.00	.00	.00	.95
VE-2021-34527	.53	.00	.00	.00	.82
VE-2018-11776	.89	.00	.00	.85	.91
VE-2023-23397	.37	.75	.00	.85	.58
VE-2017-0144	.37	.75	.00	.00	.63
VE-2021-26855	.00	.75	.00	.00	.55
VE-2021-40444	.00	.75	.00	.00	.55

Calculation (CVE-2019-0708)

U(CVE-2019-0708)=(1.00×0.40)+(1.00×0.25)+(1.00×0.15)+(0.85×0.20)U(CVE-2019-0708) = (1.00×0.40) + (1.00×0.25) + (1.00×0.15) + (0.85×0.20)U(CVE-2019-0708)=(1.00×0.40)+(1.00×0.25)+(1.00×0.15)+(0.85×0.20) =0.40+0.25+0.15+0.17=0.97= 0.40 + 0.25 + 0.15 + 0.17=0.97=0.40+0.25+0.15+0.17=0.97

Table 9. Vulnerability Priority Ranking

Ranking	CVE	Score SMART	priority
1	CVE-2021-44228	1.00	Very High
2	CVE-2020-1472	0.97	Very High
3	CVE-2019-0708	0.95	Very High
4	CVE-2022-22965	0.95	Very High
5	CVE-2021-34527	0.91	High
6	CVE-2018-11776	0.82	High
7	CVE-2023-23397	0.63	Medium
8	CVE-2017-0144	0.58	Medium
9	CVE-2021-26855	0.55	Medium
10	CVE-2021-40444	0.55	Medium

The results of the calculation show that vulnerabilities with high CVSS scores and critical impact obtain the highest SMART values. CVE-1 to CVE-4 become the top priorities because they have maximum combined values across almost all criteria.

Meanwhile, CVEs with lower CVSS scores such as CVE-6 and CVE-8 have lower priority, even though some of them have high impact, because the CVSS value contributes the largest weight (40%) in the model.

This demonstrates that the SMART method is able to integrate multiple criteria in a balanced way, resulting in a more objective vulnerability prioritization compared to using CVSS.

REFERENCES

Ahmad Heru Mujianto, Aldi Sawung Sajiyanto, & Hadi Sucipto. (2023). Implementasi Metode Simple Multi Attribute Rating Technique (Smart) Pada Sistem Informasi Penentuan Beasiswa Berbasis Website. *Jurnal Informatika Teknologi Dan Sains (Jinteks)*, *5*(2), 258–264. https://doi.org/10.51401/jinteks.v5i2.2633

Ahmadi Mehri, V., Arlos, P., & Casalicchio, E. (2022). Automated Context-Aware Vulnerability Risk Management for Patch Prioritization. *Electronics (Switzerland)*, *11*(21), 1–22. https://doi.org/10.3390/electronics11213580

Hardiyanti, D. Y., Novianti, H., & Rifai, A. (2022). Pemilihan Destinasi Objek Pariwisata Menggunakan Simple Additive Weighting (SAW). *JSI: Jurnal Sistem Informasi (E-Journal)*, *14*(2), 2934–2941. https://doi.org/10.18495/jsi.v14i2.98

Idharani, E., & Adrian, Q. J. (2025). Evaluasi Metode Smart Untuk Penentuan Bakat Anak Usia Dini. *Jurnal Pendidikan Dan Teknologi Indonesia*, *5*(8), 2193–2200. https://doi.org/10.52436/1.jpti.936

Kusnandar, A., Rochim, A. F., & Gunawan, V. (2024).

Pengukuran Tingkat Risiko dan Keamanan Informasi Menggunakan Metode FMEA Berbasis ISO/IEC 27001 pada Instansi XYZ untuk Keamanan Sistem Informasi. *Jurnal Sistem Informasi Bisnis*, *14*(4), 375–384. https://doi.org/10.21456/vol14iss4pp375-384

Sherif, E., Yevseyeva, I., Basto-fernandes, V., & Cook, A. (n.d.). *Bridging the Gap Between Security Metrics and Key Risk Indicators : An Empirical Framework for Vulnerability Prioritization*. 1–10. IEEE Access. 2026

Wunder, J., Kurtz, A., Eichenmüller, C., Gassmann, F., & Benenson, Z. (2024). Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities. *Proceedings - IEEE Symposium on Security and Privacy*, 1102–1121. https://doi.org/10.1109/SP54263.2024.00058