Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(7), 335-344
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Research and Design of Railway Security Vulnerability Management System

Dedong Zhang[1], Wenge Guo[2], Hongwei Wang[1], Lirong Hao[1]

[1]Institute of Computing Technology, China Academy of Railway Sciences Corporation Limited, Beijing, China
[2]Information Technology Institute, China Railway Taiyuan Group Co., Ltd., Taiyuan, China
Email: zhdd0411@163.com

How to cite this paper: Zhang, D.D., Guo, W.G., Wang, H.W. and Hao, L.R. (2025) Research and Design of Railway Security Vulnerability Management System. *Journal of Computer and Communications*, **13**, 335-344.
https://doi.org/10.4236/jcc.2025.137017

Received: June 16, 2025
Accepted: July 27, 2025
Published: July 30, 2025

Abstract

Based on both domestic and overseas research on vulnerability management, considering the actual pain point and needs of railway enterprises, a security vulnerability management system was proposed. The system has achieved the collection, filtering, and standardization of vulnerability information, as well as the management of the mapping relationship between vulnerabilities and assets. The article analyzes and designs the construction principles, objectives, overall architecture, and functional structure of the system. The system can be applied to security warning and vulnerability management, and has brought satisfactory effects in practice.

Keywords

Security Vulnerability, Vulnerability Information Management, Vulnerability Lifecycle, Vulnerability Connection

1. Introduction

With the swift advancement of computing and networking technologies, the global internet's scale has expanded rapidly, and cyberspace is becoming increasingly intelligent and complex. While the internet brings us convenience, its cybersecurity issues are gradually becoming more prominent. Security vulnerabilities are the core of information security technology, most of the network attacks are often initiated exploiting vulnerabilities [1]. According to the "2024 Annual Cybersecurity Vulnerability Analysis Report", there were 44,957 new cybersecurity vulnerabilities globally in 2024, representing an increase of over 50% compared to 2023 [2]. In view of this, how to effectively collect and manage vulnerabilities has become an important issue in the field of network security. Existing vulnerability databases such as Common Vulnerabilities & Exposures (CVE) [3] [4] and China

National Vulnerability Database of Information Security (CNNVD) provide basic vulnerability information, but they show obvious deficiency in terms of data timeliness, analysis depth and sharing mechanisms.

As an important component of the country's critical information infrastructure, the cybersecurity of railways is directly related to the national economic lifeline and public safety [5]. With the in-depth advancement of railway informatization, railway information systems have been widely applied in key business areas such as train control, dispatching command, passenger ticket sales, and passenger services. There are numerous challenges in railway vulnerability management. Firstly, the railway system comprises multiple systems such as the signaling system, communication system, dispatching system, and ticketing system. These systems are interdependent, forming a complex network. Any security issue in any of these links may affect the stability of the entire system. Secondly, the railway system comprises many operational equipment, which have long service cycles and slow replacement rates. These systems have many security vulnerabilities. Thirdly, the railway supply chain is complex, involving numerous suppliers. The heterogeneity and universality of equipment pose challenges to the management of security vulnerabilities. The railway system has extremely high requirements for real-time performance and reliability. Traditional vulnerability management methods and vulnerability update mechanisms can affect the normal operation of the system and increase the difficulty of vulnerability remediation.

Therefore, we should establish a network security vulnerability management system for railway. It is beneficial for railway management departments to analyze the number and types of vulnerabilities, and grasp the overall situation of railway vulnerabilities; It is beneficial to understand the vulnerabilities of the system and take timely protective measures; It is beneficial to share vulnerability management and remediation techniques, thereby enhancing the level of vulnerability management.

2. Current Situation of Railway Security Vulnerability

2.1. Vulnerability Type and Distribution

The railway system encompasses a vast array of hardware and software devices or systems, including network equipment, security devices, operating systems, databases, middleware, and business application software. There are various types of security vulnerabilities in these systems. According to statistics, these security vulnerabilities are primarily concentrated at the middleware, database, and operating system. Once exploited by attackers, these vulnerabilities are highly likely to cause serious consequences such as data leakage and service interruptions, posing a significant threat to the normal operation of railway business.

2.2. Status of Vulnerability Management

There are several issues in the management of railway network security vulnerabilities.

Firstly, it is difficult to detect all vulnerabilities because of the complexity of

assets. The railway system is large-scaled, with equipment provided by numerous manufacturers. The equipment exhibits significant differences in design philosophy, technical standards and implementation methods. Furthermore, the railway system encompasses software such as operating systems, middleware, and various information systems. This software is based on different development platforms and frameworks, further increasing the difficulty of vulnerability detection. At the same time, a wide variety of software is running on this equipment, including operating systems, middleware, and information systems. These software applications are built on diverse development platforms and frameworks, and it further increases the difficulty of vulnerability detection.

Secondly There are various types of vulnerabilities. Vulnerabilities in the railway system are widespread, including operating system vulnerabilities, application vulnerabilities and middleware vulnerabilities. In terms of the operating system, there may be vulnerabilities such as buffer overflow and privilege escalation. In terms of applications, vulnerabilities such as SQL injection and cross-site scripting attacks are prone to occur. In terms of the database and middleware, vulnerabilities arise due to outdated versions. Different types of vulnerabilities have their respective formation mechanisms, harm methods, and technical characteristics.

Thirdly, vulnerabilities change rapidly. The operational environment of the railway system is constantly evolving, encompassing upgrades to application system versions, replacements of hardware equipment, adjustments to network configurations, and more. These changes have the potential to introduce new vulnerabilities.

Finally, it is difficult to set up a testing environment for vulnerability validation. Some business systems are crucial to railway operations, and normal business operations cannot be affected by vulnerability detection. Therefore, to identify vulnerabilities, it is necessary to establish a testing environment that is identical to the actual operational environment. However, due to the complexity of the railway business system, establishing a testing environment is extremely challenging. It is difficult to implement some vulnerability remediation solutions within the system.

3. Design Principles and Objectives of Vulnerability Management System

3.1. Design Principles

1) Compatibility principle

Standardized and normative data is more conducive to management, sharing and circulation. The railway vulnerability management system should be fully compatible with influential vulnerability standards both domestically and internationally, such as CVE and CNNVD, and should be capable of supporting unified management of vulnerability [6]-[8] data with different formats and different sources. Meanwhile, the system is compatible with vulnerability scanning devices

from different manufacturers.

2) Comprehensiveness principle

The railway vulnerability database should encompass vulnerabilities of software and hardware such as operating systems, databases, middleware, network devices, and security devices. It should track the latest vulnerability information both domestically and internationally, and promptly update the vulnerability database accordingly [9] [10]. The vulnerability database should provide detailed vulnerability information, including at least the affected versions, potential threats, whether they can be exploited, and corresponding solutions.

3) Security principle

System design should consider aspects such as technological progressiveness, data confidentiality, and system security. The system should encrypt important data such as user identities, device assets, and vulnerability information to ensure that the data is not illegally misused or leaked. The system should adopt fine-grained access control measures to grant access to system resources based on user permissions.

3.2. Objectives of Vulnerability Management System

1) Establish a platform for vulnerability information sharing and exchange, providing users with authoritative, standardized, and timely security vulnerability information, accurately analyzing the impact of vulnerabilities, and issuing risk warnings for vulnerabilities.

2) Establish an efficient vulnerability management mechanism. The system can evaluate the vulnerability levels, provide vulnerability remediation priority strategy and guide users Guide users to repair vulnerabilities. That can meet the needs of system operation and maintenance.

3) Establish a vulnerability remediation plan sharing mechanism. It aids in the closed-loop management of vulnerabilities.

4. Systems Design

4.1. System Architecture

The railway network security vulnerability management system can be divided into the following layers according to its hierarchical structure [11] [12]: data collection layer, interface layer, data layer, support layer, business layer, and presentation layer. Its architecture is shown in **Figure 1**.

Display layer: Displays vulnerability information, asset information, early warning information, and statistical analysis, providing users with access to data maintenance, data querying, vulnerability management, work order handling, and system management.

Business layer: Provides data for the presentation layer and performs data processing. It mainly includes functions such as asset management, vulnerability management, detection task management, threat warning management, work order management, and statistical reporting.

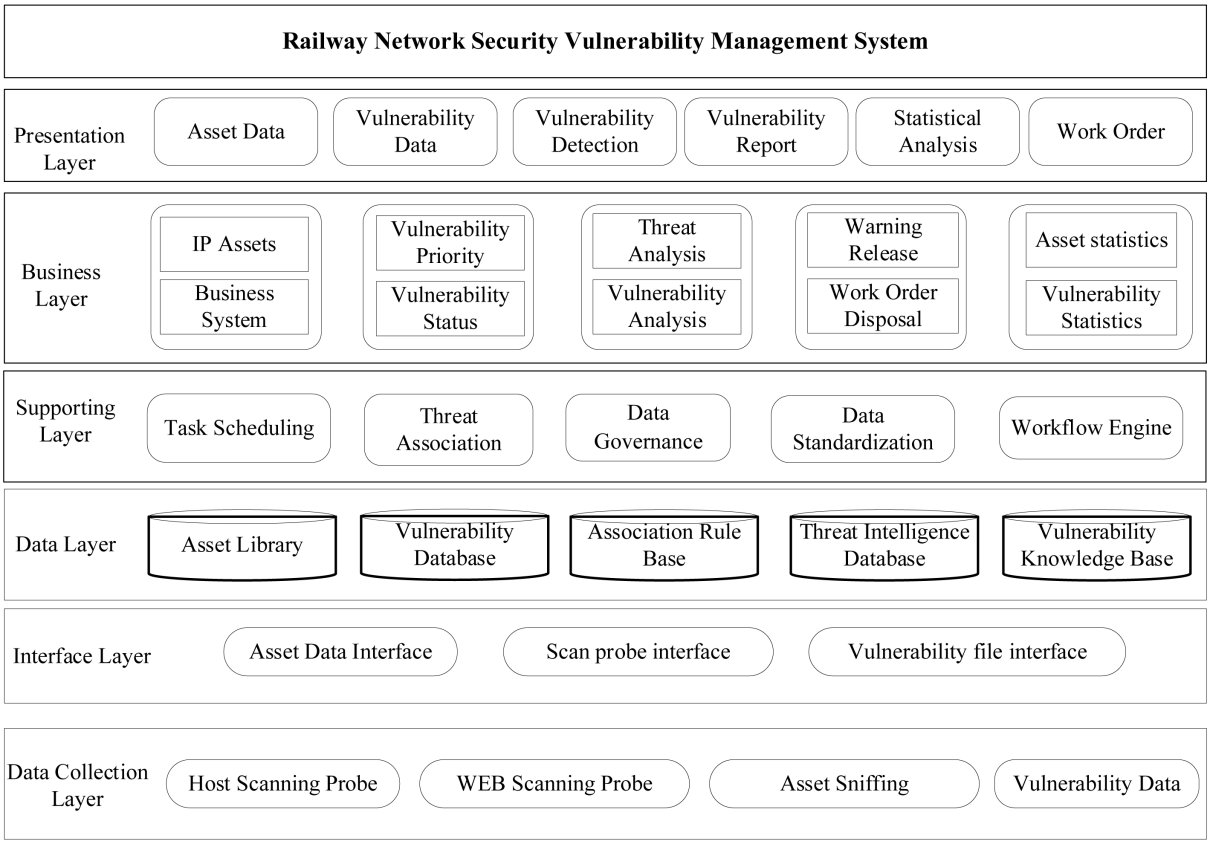

Figure 1. System architecture.

Support layer: Provides data standardization, data security, data caching, data analysis, and data application services for the system, mainly including service modules such as task scheduling, data caching, threat warning analysis, data governance, data security, and data reporting.

Data layer: It primarily involves centralized storage of asset data, vulnerability data, CNNVD/CVE standard vulnerability data, threat intelligence, vulnerability solutions, etc., including asset library, vulnerability library, association rule library, threat intelligence database and vulnerability knowledge base.

Interface layer: responsible for data parsing, data cleaning, and normalization of vulnerability data, converting it into a unified data format.

Data collection layer: Primarily used for obtaining vulnerability data and asset data.

4.2. System Composition

The system includes four parts: vulnerability data collection, vulnerability data handling and storage, vulnerability process management, and vulnerability data display [13] [14]. The system composition is shown in **Figure 2**.

1) Vulnerability data collection. At this stage, the system mainly completes data collection, data format normalization, and data filtering. It achieves unified management of vulnerability scanning probes from different vendors by driving the

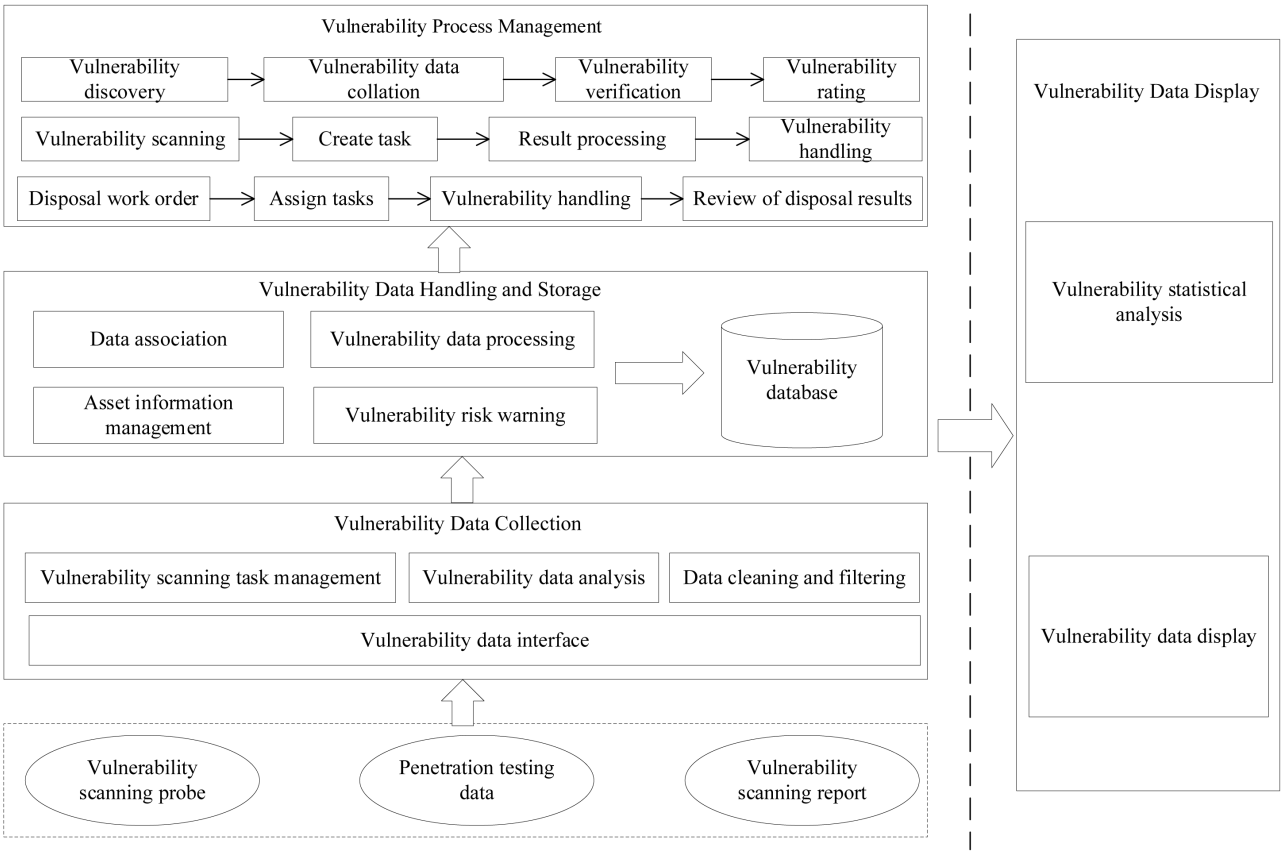

Figure 2. System composition.

vulnerability data API interface. The system can collect the vulnerability data from vulnerability scanning probes, penetration testing, network security inspection, etc. Then, clean and filter the vulnerability data, remove any duplicates, and identify the vulnerabilities that require attention.

2) Vulnerability data handling and storage. It includes functions such as asset management, heterogeneous data processing, data correlation, and vulnerability risk analysis. The original vulnerability data is unified and standardized, and then the standardized vulnerability data is associated with asset data, patch data, and vulnerability knowledge base. At the same time, the system compares information such as assets, equipment, software vendors, and software versions with vulnerability data to analyze potential vulnerability warning information and issue alerts.

3) Vulnerability process management. It includes the vulnerability discovery process, the vulnerability scanning process and the vulnerability handling process.

The vulnerability discovery process includes various stages such as vulnerability discovery, vulnerability review, vulnerability data processing, vulnerability verification, vulnerability classification, and vulnerability storage.

The vulnerability scanning process. The system drives the vulnerability scanning equipment to execute the vulnerability scanning task. It correlates vulnerability data with CNNVD and CVE data, and can conduct risk assessment on the vulnerability data based on CVSS scores [15], asset attributes, vulnerability attributes.

The vulnerability handling process. Based on vulnerability and asset information, the system creates vulnerability remediation work orders and distributes them to relevant cybersecurity personnel. Additionally, the system can provide vulnerability remediation methods or patch information, and verify and review the remediation results.

The vulnerability handling process is shown in **Figure 3**.

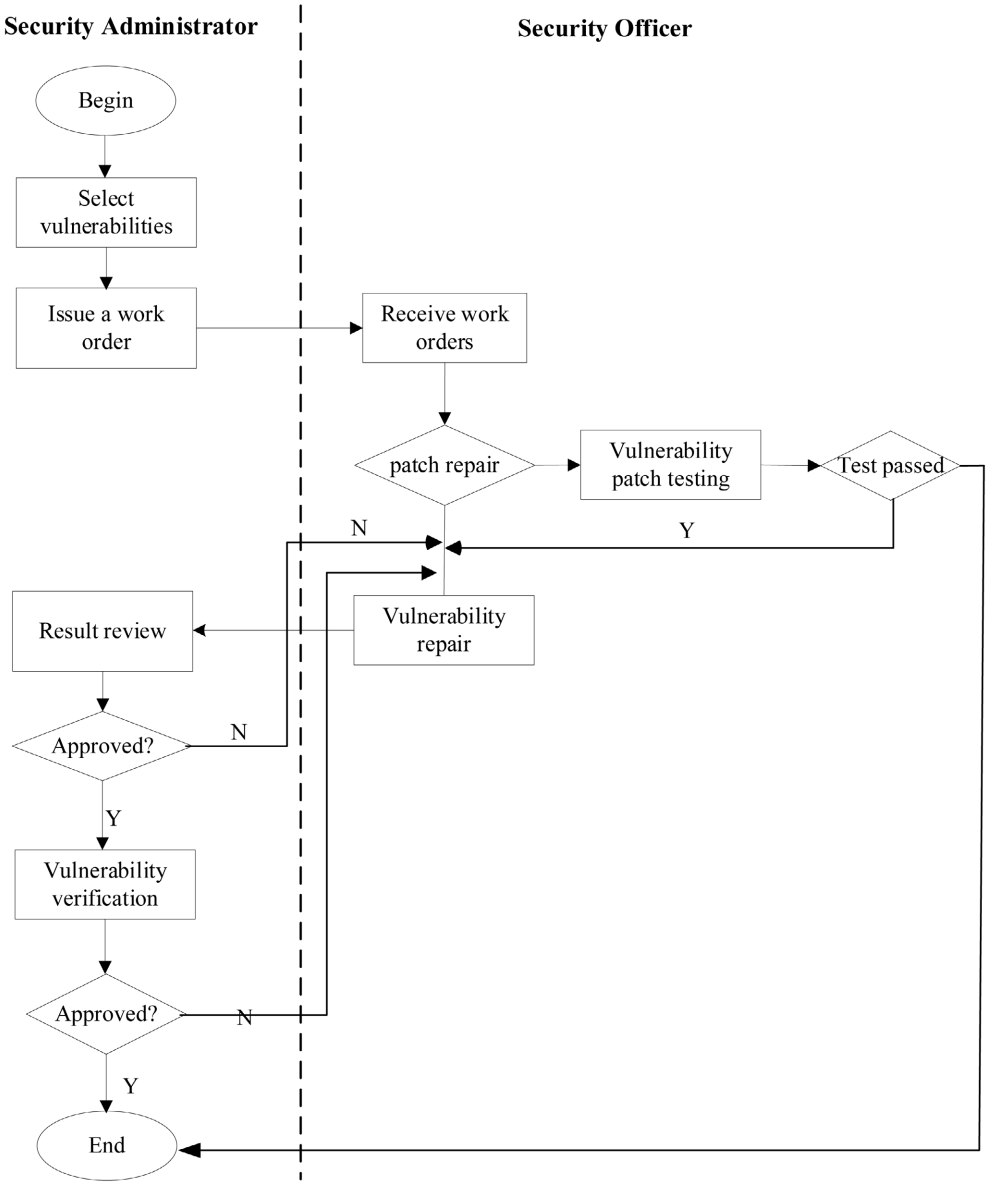

Figure 3. Vulnerability handling process.

4) Vulnerability data display.

Vulnerability query: The system can conduct queries based on conditions such as vulnerability type, risk level, release time, and affected assets.

Vulnerability display: the system can display information including basic vulnerability information, detection information, affected assets, remediation plans, etc.

4.3. System Function

The system mainly includes six functional modules: asset management, vulnerability management, detection management, patch management, work order management, and statistical analysis [16] [17], as shown in **Figure 4**.

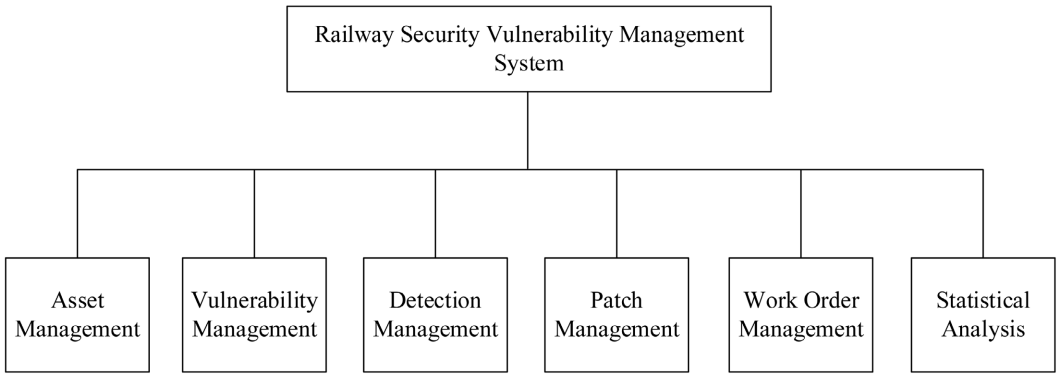

Figure 4. System function.

1) Asset Management.

Asset data can be added, deleted, and modified through the system. At the same time, the system provides multiple query functions, supporting both precise and fuzzy queries.

2) Vulnerability management

Vulnerability management is divided into four stages: vulnerability collection, vulnerability assessment, vulnerability handling, and vulnerability retesting. The system can conduct periodic vulnerability scanning on assets to achieve comprehensive and effective monitoring and management of vulnerabilities

3) Detection Management

The system integrates vulnerability scanning devices from multiple vendors and brands, and organizes these devices into a resource pool. Based on the vulnerability scanning scenarios and environments, strategies for probe devices in the resource pool can be set.

4) Patch Management

The system conducts unified collection and display of patches, establishes associations between vulnerabilities and patches, and provides functions such as patch query and download.

5) Work Order

Vulnerability fixes can be managed through work orders. Security administrators create work orders, select vulnerabilities that need to be fixed, and set the urgency level and completion time. Vulnerability handling can be monitored through work order management.

6) Statistical Analysis

The system provides functions for asset information statistics and vulnerability information statistics.

Asset information statistics primarily encompasses statistical functions across

the following dimensions:

a) Ranking of asset risk values and vulnerability counts;

b) Statistics on asset vulnerabilities, comparing year-on-year and month-on-month;

c) Risk value and vulnerability distribution statistics of individual assets.

Vulnerability information statistics mainly includes the following dimensions:

a) Support the analysis of the impact scope of vulnerability distribution, and conduct statistics based on the risk value of affected assets;

b) Support ranking of vulnerability counts discovered on a monthly, quarterly, and annual basis;

c) Support ranking of vulnerability levels (high, medium, low).

5. Conclusion

Vulnerabilities are the primary source of many malicious attacks. It is imperative to standardize the management of vulnerabilities and establish a railway network security vulnerability management system. The system is based on asset management and centered around vulnerability management. A standardized description of railway vulnerability formats is provided based on the CNNVD/CVE vulnerability database. The vulnerability is gathered by using various technologies and methods firstly, and then it is filtered, merged, and standardized. The system provides vulnerability analysis functionality and a mapping relationship between assets and vulnerabilities and achieves full lifecycle management for vulnerabilities, including discovery, assessment, handling and remediation.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Cao, X.D., Huang, Z.Q., Chen, Y.J., *et al.* (2024) An Overview of Research on Vulnerability Database Construction and Application. *Chinese Journal of Computers*, **47**, 1082-1119.

[2] https://blog.csdn.net/2301_76786857/article/details/145962475

[3] Fucci, D., Di Penta, M., Romano, S., *et al.* (2025) Augmenting Software Bills of Materials with Software Vulnerability Description: A Preliminary Study on GitHub.

[4] Ping, L., Jin, S. and Yang, X. (2012) Research on Software Security Vulnerability Detection Technology. *Proceedings of* 2011 *International Conference on Computer Science and Network Technology*. https://doi.org/10.1109/ICCSNT.2011.6182335

[5] Zhang, S., Wang, W., Tian, Z., *et al.* (2024) Research on Railway 5G-R Network Security Technology. *China Railway*, No. 8, 62-68.

[6] Chen, Q., He, J., and Lu, J. (2024) Application of Black Box Genetic Algorithm in Network Security Vulnerability Mining. *Proceedings of SPIE*, **13073**, 4. https://doi.org/10.1117/12.3026709

[7] Shaoliang, C. (2019) Design of Network Security Vulnerability Scanning System Based on Deep Learning in the Equal Guarantee 2.0 Era. *China Computer & Communication*.

[8] Yang, G., Wen, T. and Zhang, Y. (2015) Design and Implementation of Android Vulnerability Database. *Netinfo Security*, No. 9, 240-244.

[9] Fang, J., Li, Y. and Li, Y. (2016) Analysis and Research on Security Vulnerability Database. *International Conference on Mechanical*. https://doi.org/10.2991/itoec-16.2016.26

[10] Zhang, Y., Wu, S., Liu, Q., *et al*. (2011) Design and Implementation of National Security Vulnerability Database. *Journal on Communications*, **32**, 93-100.

[11] Li, Y. and Li, J. (2020) Intelligent Detection System of Asset Security Vulnerability Hidden Danger under Multiple and Heterogeneous Web Network. *Journal of Physics Conference Series*, **1684**, 012005. https://doi.org/10.1088/1742-6596/1684/1/012005

[12] Zhang, S. and Jiang, K. (2016) Vul Tracker Platform for Vulnerability Management and Automatic Tracking. *J. Huazhong Univ. of Sci. & Tech*. (*Natural Science Edition*), **44**, 7-10.

[13] Chalvatzis, I, Karras, D.A. and Papademetriou, R.C. (2019) Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment. 2019 *IEEE International Conference on Artificial Intelligence and Computer Applications* (*ICAICA*). https://doi.org/10.1109/ICAICA.2019.8873438

[14] Xinna, S. (2018) Analysis and Research of Computer Network security Vulnerability. Electronic Test.

[15] He, D., Deng, Z., Zhang, Y., *et al*. (2020) Smart Contract Vulnerability Analysis and Security Audit. *IEEE Network*, No. 99, 1-7.

[16] Zhou, P., Wu, Y. and Zhao, C. (2022) Identify Linux Security Vulnerability Fix Patches Automatically. *Journal of Computer Research and Development*, **59**, 197-208.

[17] Yuan, L., Bai, Y., Xing, Z., *et al*. (2021) Predicting Entity Relations Across Different Security Databases by Using Graph Attention Network. *Proceeding of the* 2021 *IEEE* 45*th Annual Computers, Software, and Applications Conference*, Madrid, Spain, 834-843. https://doi.org/10.1109/COMPSAC51774.2021.00116