Journal scientific and applied research, vol. 28, 2025
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

A COMPARATIVE ANALYSIS OF MODERN VULNERABILITY SYSTEMS AND DATABASES

Petar Kr. Boyanov

DEPARTMENT OF COMMUNICATION AND COMPUTER ENGINEERING AND SECURITY TECHNOLOGIES, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712, 115, UNIVERSITETSKA STR.,
E-MAIL: petar.boyanov@shu.bg

ABSTRACT: *This scientific article examines and compares several modern vulnerability management systems and databases, such as CVE, CWE, EUVD, NVD, and OSVDB. The goal is to understand how these resources differ in scope, structure, and interoperability. In the article of the analysis, particular attention is paid to platforms like MITRE's frameworks, Exploit-DB, and Rapid7-DB, as well as to international initiatives such as Japan's JVN project. The scientific study also reviews the scoring models they employ, mainly CVSS, and considers alternatives like VEDAS. Overall, the results highlight how each system contributes differently to strengthening cybersecurity practices and how they can complement one another in real-world defense strategies.*

KEY WORDS: *CVE, CVSS, CWE, EUVD, Exploit-DB, Japan Vulnerability Notes (JVN), MITRE, NVD, OSVDB, RAPID7-DB, VEDAS.*

1. Introduction

The modern digital environment faces a constant and evolving wave of software vulnerabilities, which continue to threaten global information security. Because of this, effective vulnerability management has become one of the key components of contemporary cybersecurity, requiring consistent, structured, and data-driven approaches. To achieve this, the process depends on a broad ecosystem of specialized databases and systems that help security professionals identify, categorize, and prioritize software flaws. These repositories form the essential knowledge base for the global cybersecurity community, supporting coordinated defense activities and faster mitigation of threats.

Among the most influential initiatives in this field is the Common Vulnerabilities and Exposures (CVE) system [1,11,12], maintained by MITRE, which assigns standardized identifiers to publicly disclosed vulnerabilities. The National Vulnerability Database (NVD), built upon the CVE list [1,11,12], expands this information by adding analytical data such as severity ratings through the Common Vulnerability Scoring System (CVSS). In parallel, the Common Weakness Enumeration (CWE) offers a conceptual framework for describing the underlying causes of software weaknesses instead of focusing only on specific cases.

The vulnerability management ecosystem extends beyond these core systems and includes a number of other important sources. For example, the now-retired Open Source Vulnerability Database (OSVDB) represented an early, community-based initiative to document security issues [4,18]. Modern platforms such as Exploit-DB and Rapid7-DB remain highly valuable because they focus on exploit code and proof-of-concept demonstrations that show how specific vulnerabilities can be practically used [5]. On an international level, systems like Japan Vulnerability Notes (JVN) adapt global vulnerability data to the needs of the Japanese software market [8,17]. In addition, research-oriented models such as VEDAS introduce data-driven approaches to evaluating vulnerabilities.

Although these platforms share a common purpose, they differ significantly in scope, data sources, and operational design. This diversity can make it difficult for organizations [15] to develop a unified and effective vulnerability management strategy. The present article therefore offers a systematic comparative study of these databases and systems, aiming to clarify their specific functions, overlaps, and relative strengths, and to provide guidance for both researchers and practitioners.

The increasing number of reported vulnerabilities each year makes manual evaluation nearly impossible, which means that automated prioritization has become essential. Yet, variations in data structures, update schedules, and scoring models across platforms frequently cause integration issues and inconsistent interpretations. As a result, a vulnerability considered critical in one system might appear less urgent in another, leading to uneven security responses. Moreover, the discontinuation of projects such as OSVDB highlights the dynamic and unstable nature of this field, as well as the need for a better understanding of sustainable alternatives. A structured comparison of current systems is therefore necessary to inform tool selection, improve data integration, and enhance the overall efficiency of organizational vulnerability management.

The content of this academic work is intended for research and instructional applications. Any unauthorized or unethical use of the presented material falls outside the author's scope of responsibility.

2. Related work

The body of academic research addressing vulnerability management systems reveals a wide range of interconnected investigations that together outline how modern flaw-tracking practices have evolved. Early studies [1] laid the conceptual groundwork for understanding the development of vulnerability cataloging, showing how the CVE system [1,11,12] created a standardized terminology that allows consistent communication between different repositories. Building on this foundation, later analyses such as [2] examined the limitations of the CVSS scoring methodology within databases that document contemporary cyberattacks.

Parallel lines of inquiry have explored the internal diversity of vulnerability databases. The review of OSVDB's operational history in [4] provides valuable insight into community-driven monitoring efforts while [10] offers a detailed structural assessment of how the NVD manages and processes vulnerability intelligence. Research focused on geographically tailored systems such as studies [8] and [17] has shown how regional initiatives like Japan's JVN adapt global vulnerability information for local use. The changing nature of distributed vulnerability repositories and their associated challenges is further discussed in [21].

Researchers have also examined the specialized functions of individual repositories. Study [5] analyzes the contribution of platforms such as Exploit-DB in improving access to penetration testing resources, whereas [19] discusses how proprietary databases like Rapid7-DB are integrated into defensive architectures. Work in [16] introduces automated assessment mechanisms through the VEDAS model, illustrating a broader trend toward algorithmic prioritization.

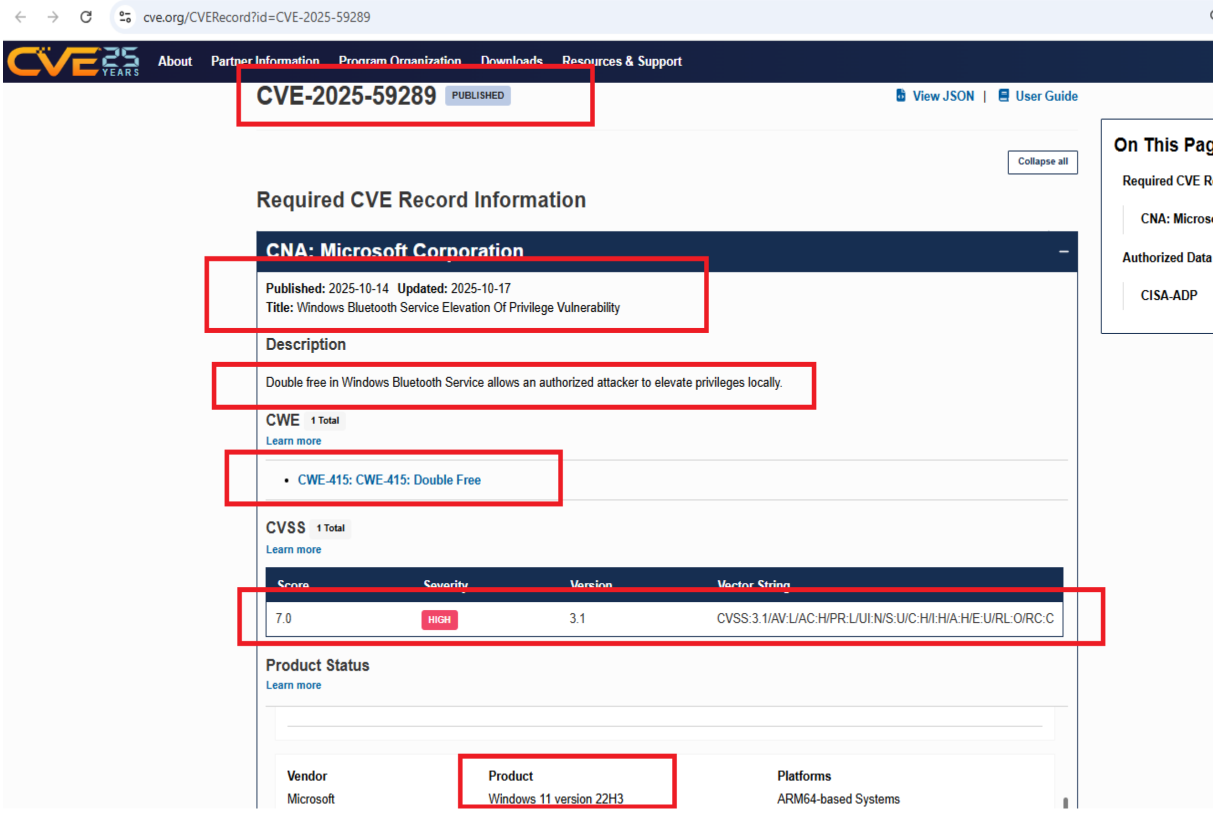
Methodological contributions include [13]'s quantitative evaluation of vulnerability prioritization metrics and [7]'s comparison of national database strategies. Broader ecosystem perspectives are presented in [6] and [14], which discuss MITRE's central role in shaping cybersecurity standards and the interaction between the ATT&CK and CWE frameworks. In addition, [20] explores the application of CWE-based analysis to proactive software defense, while [3] highlights CWE's essential role in secure software development lifecycles.

In summary, existing studies offer significant insight into individual elements of the vulnerability management ecosystem [1,11], yet they often address these components separately [2,13]. What remains missing is a comprehensive comparative perspective that systematically examines the scope [7,8,17,20], data integrity, operational focus, and potential synergy among core vulnerability databases, exploit-oriented repositories [5,15,18], international systems, and experimental research frameworks.

3. Experiment

The scientific experiments in this article in a controlled virtual computer environment were conducted.

The Common Vulnerabilities and Exposures (CVE) list serves as the basic dictionary for the cybersecurity community, offering standardized identifiers for publicly known software flaws. Its purpose is to provide a common language that enables various organizations and security tools [11] to exchange information clearly and consistently. Each CVE entry consists of a unique identifier that includes the year of disclosure and a sequential number. Importantly, a CVE record itself does not include technical analysis, risk ratings, or remediation details. Instead, it acts as a reference point that links data across multiple security platforms and repositories. The program is maintained by the MITRE Corporation and funded by the U.S. Department of Homeland Security. Today, obtaining a CVE ID [1,11,12] has become a standard step in the responsible disclosure process for nearly all security vulnerabilities. Without this consistent naming system, information sharing across the global security ecosystem would be fragmented and inefficient. Though a U.S.-based initiative, CVE's adoption is worldwide, forming the base layer upon which many other databases are built. Fig. 1 shows the detailed information about vulnerability record - CVE-2025-59289.



CVE-2025-59289 PUBLISHED

Required CVE Record Information

CNA: Microsoft Corporation

Published: 2025-10-14 **Updated:** 2025-10-17
Title: Windows Bluetooth Service Elevation Of Privilege Vulnerability

Description

Double free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.

CWE 1 Total
Learn more

- CWE-415: CWE-415: Double Free

CVSS 1 Total
Learn more

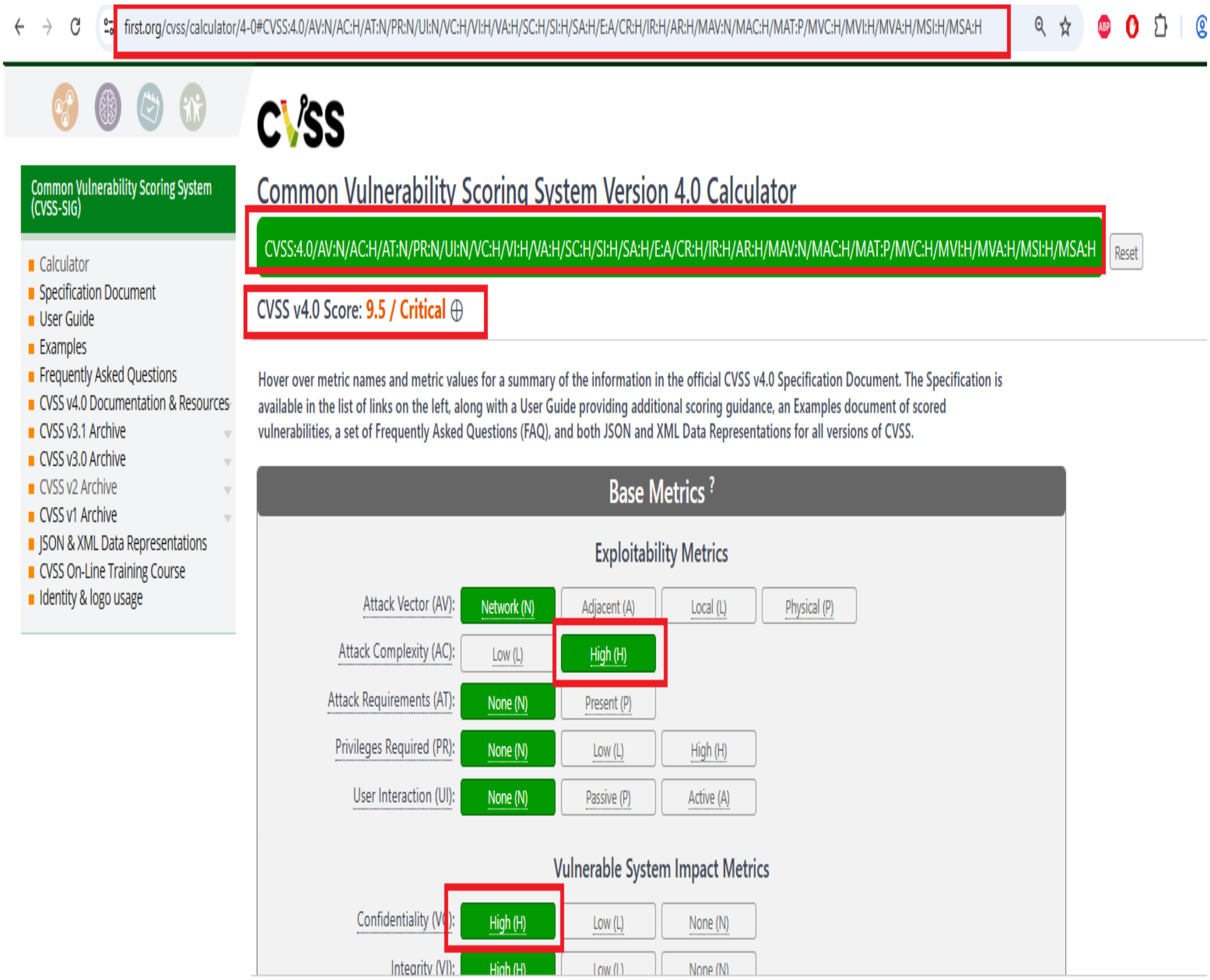
Score	Severity	Version	Vector String
7.0	HIGH	3.1	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Product Status
Learn more

Vendor	Product	Platforms
Microsoft	Windows 11 version 22H3	ARM64-based Systems

Fig. 1. CVE vulnerability database

The Common Vulnerability Scoring System (CVSS) provides an open and standardized method for assessing the severity of software vulnerabilities. It translates complex technical properties into a numerical score that reflects the potential risk level. The framework includes three metric groups: base metrics describing the fundamental characteristics of a flaw [13]; temporal metrics, which account for time-dependent factors like the availability of exploit code; and environmental metrics, which let organizations [15] adjust scores to match their specific systems and risk tolerance. The base score primarily measures exploitability and potential impact [2,13], while the temporal and environmental factors add contextual relevance. The final value, between 0.0 and 10.0, gives a concise view of a vulnerability's danger [13]. However, this number is not an absolute measure of risk—it should be treated as one input in a broader risk management process [2,13]. CVSS is governed by the Forum of Incident Response and Security Teams (FIRST), whose stewardship ensures the model evolves alongside industry needs. Its widespread use has made it the de facto standard for prioritizing mitigation across the cybersecurity field [2,13]. Fig. 2 shows a custom made vulnerability 4.0 calculator with score of 9.5 critical points.



first.org/cvss/calculator/4-0#CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:A/CR:H/IR:H/AR:H/MAV:N/MAC:H/MAT:P/MVC:H/MVI:H/MVA:H/MSI:H/MSA:H

Common Vulnerability Scoring System Version 4.0 Calculator

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:A/CR:H/IR:H/AR:H/MAV:N/MAC:H/MAT:P/MVC:H/MVI:H/MVA:H/MSI:H/MSA:H

CVSS v4.0 Score: 9.5 / Critical

Hover over metric names and metric values for a summary of the information in the official CVSS v4.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, a set of Frequently Asked Questions (FAQ), and both JSON and XML Data Representations for all versions of CVSS.

Base Metrics

Exploitability Metrics

Attack Vector (AV): Network (N)

Attack Complexity (AC): High (H)

Attack Requirements (AT): None (N)

Privileges Required (PR): None (N)

User Interaction (UI): None (N)

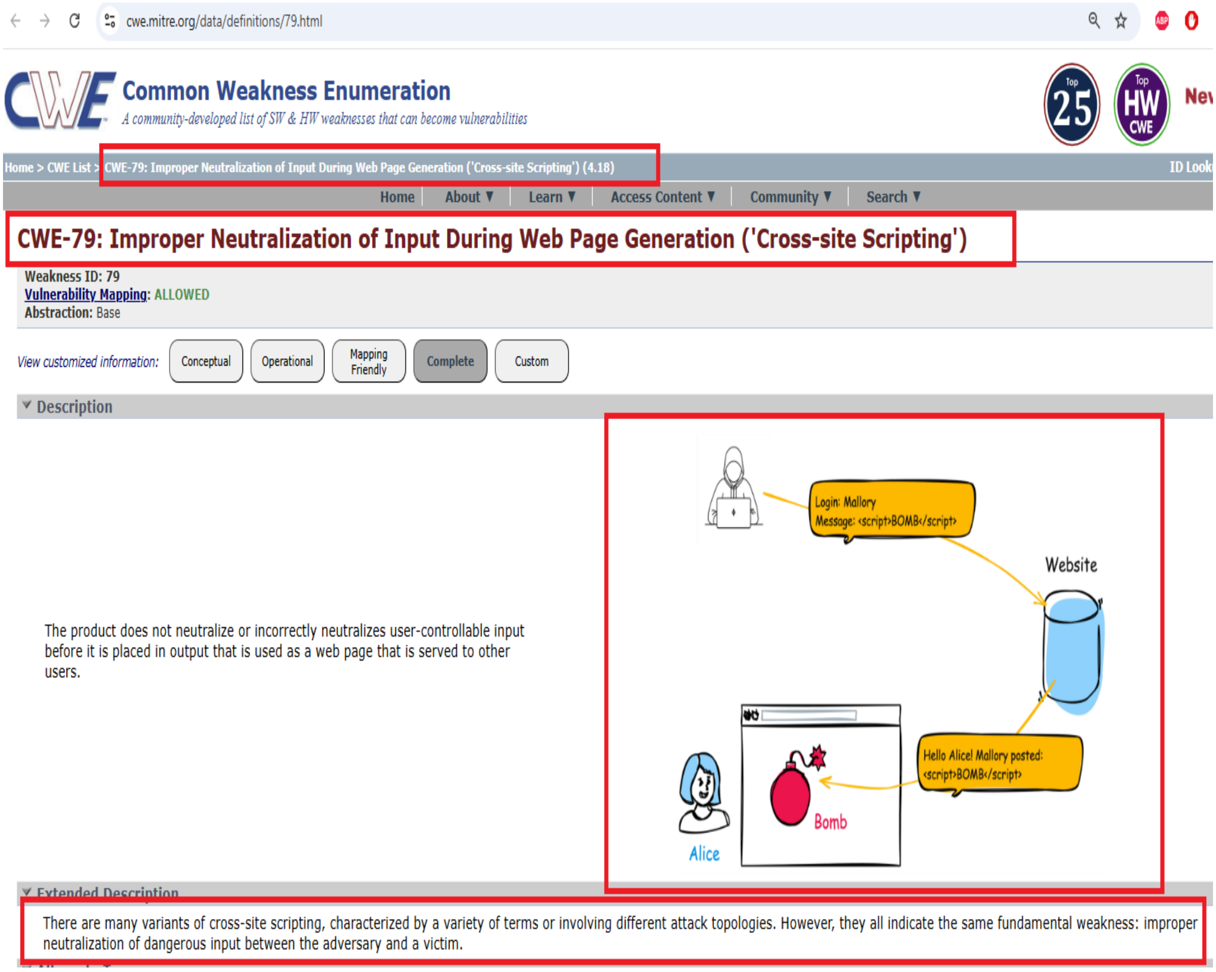
Vulnerable System Impact Metrics

Confidentiality (VC): High (H)

Integrity (VI): High (H)

Fig. 2. CVSS vulnerability calculator

The Common Weakness Enumeration (CWE) differs from CVE by focusing on categories of software and hardware design weaknesses rather than specific vulnerability instances [3,14]. It serves as a taxonomy that identifies recurring programming and architectural errors that can lead to security issues. By emphasizing the underlying causes [3,14], CWE encourages developers to prevent flaws before they manifest as exploitable vulnerabilities. The framework is community-driven and provides a shared vocabulary for developers, architects, and security professionals. Each entry describes patterns such as buffer overflows or cross-site scripting in abstract terms, independent of any product or CVE [3,14]. CWE is used extensively in secure development lifecycles, code analysis tools, and educational materials [3,14]. Many organizations employ the taxonomy [20] to evaluate their coding practices and to identify recurring weakness trends. In this sense, CWE offers a blueprint for proactive security—helping teams to "build security in" from the start [20,3,14]. Fig. 3 illustrates the cyber-attack XSS with its vulnerability record information.


cwe.mitre.org/data/definitions/79.html
Common Weakness Enumeration
A community-developed list of SW & HW weaknesses that can become vulnerabilities
Top 25
Top HW CWE
Nev
Home > CWE List > CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (4.18)
ID Look
Home
About ▼
Learn ▼
Access Content ▼
Community ▼
Search ▼

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Weakness ID: 79
Vulnerability Mapping: ALLOWED
Abstraction: Base

View customized information:
Conceptual
Operational
Mapping Friendly
Complete
Custom
▼ Description

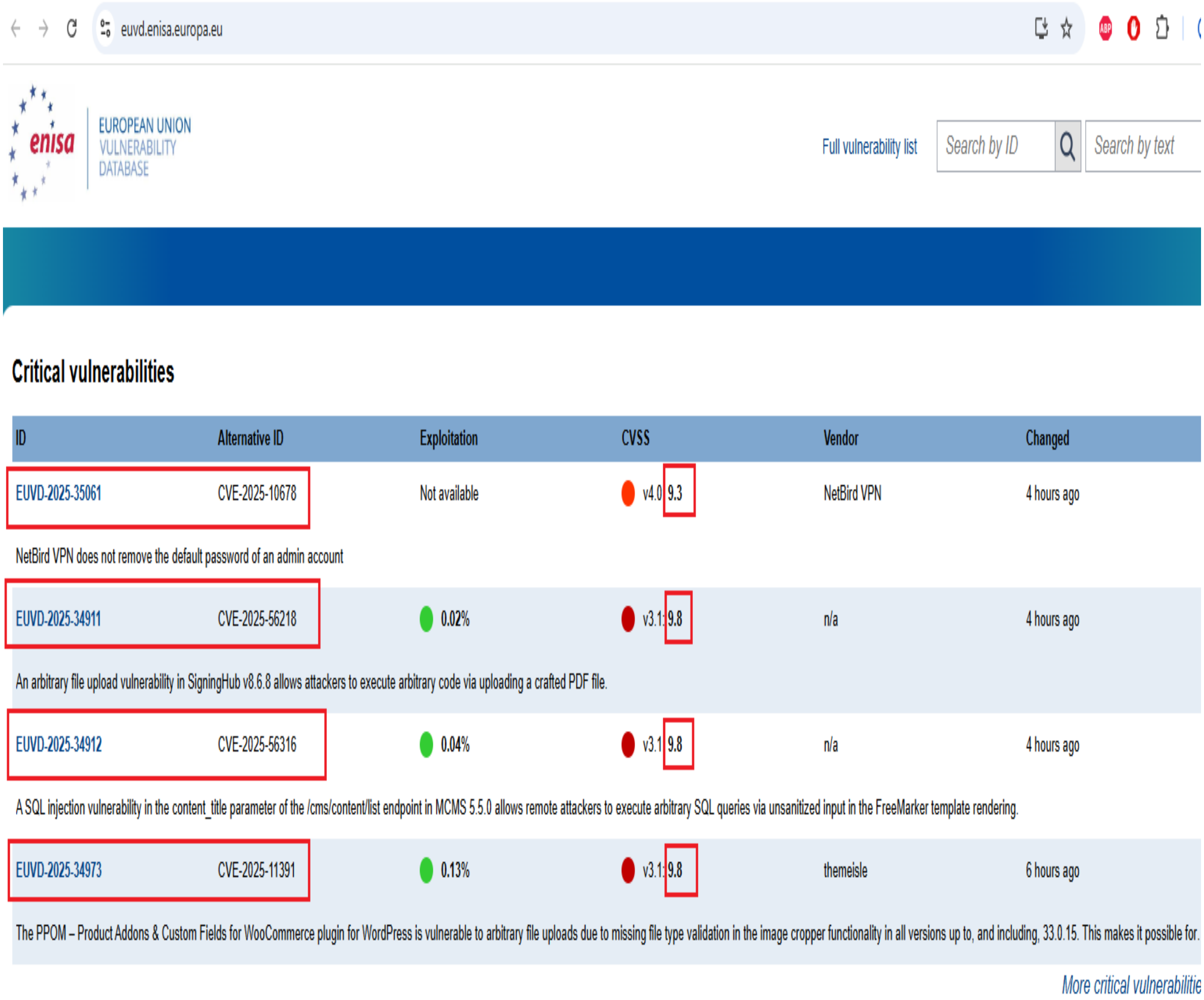
The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Login: Mallory
Message: <script>BOMB</script>
Website
Hello Alice! Mallory posted: <script>BOMB</script>
Bomb
Alice
▼ Extended Description

There are many variants of cross-site scripting, characterized by a variety of terms or involving different attack topologies. However, they all indicate the same fundamental weakness: improper neutralization of dangerous input between the adversary and a victim.

Fig. 3. CWE vulnerability database

The European Union Agency for Cybersecurity (ENISA) maintains a database of vulnerabilities designed to address European regulatory and operational priorities [21]. This resource often focuses on threats that affect critical infrastructure within the EU and supports policy-making, certification efforts, and incident response coordination. Beyond serving as a data repository, ENISA's platform provides analysis and contextual reports that guide national cybersecurity agencies and decision-makers [21]. The system's curated approach helps identify vulnerabilities that could have the most significant impact on the European digital market. It therefore functions both as a technical and strategic tool for governments, CERTs, and operators of essential services [21], reinforcing Europe's goal of digital resilience and strategic autonomy. Fig. 4 presents several critical vulnerabilities that are detected in 2025.



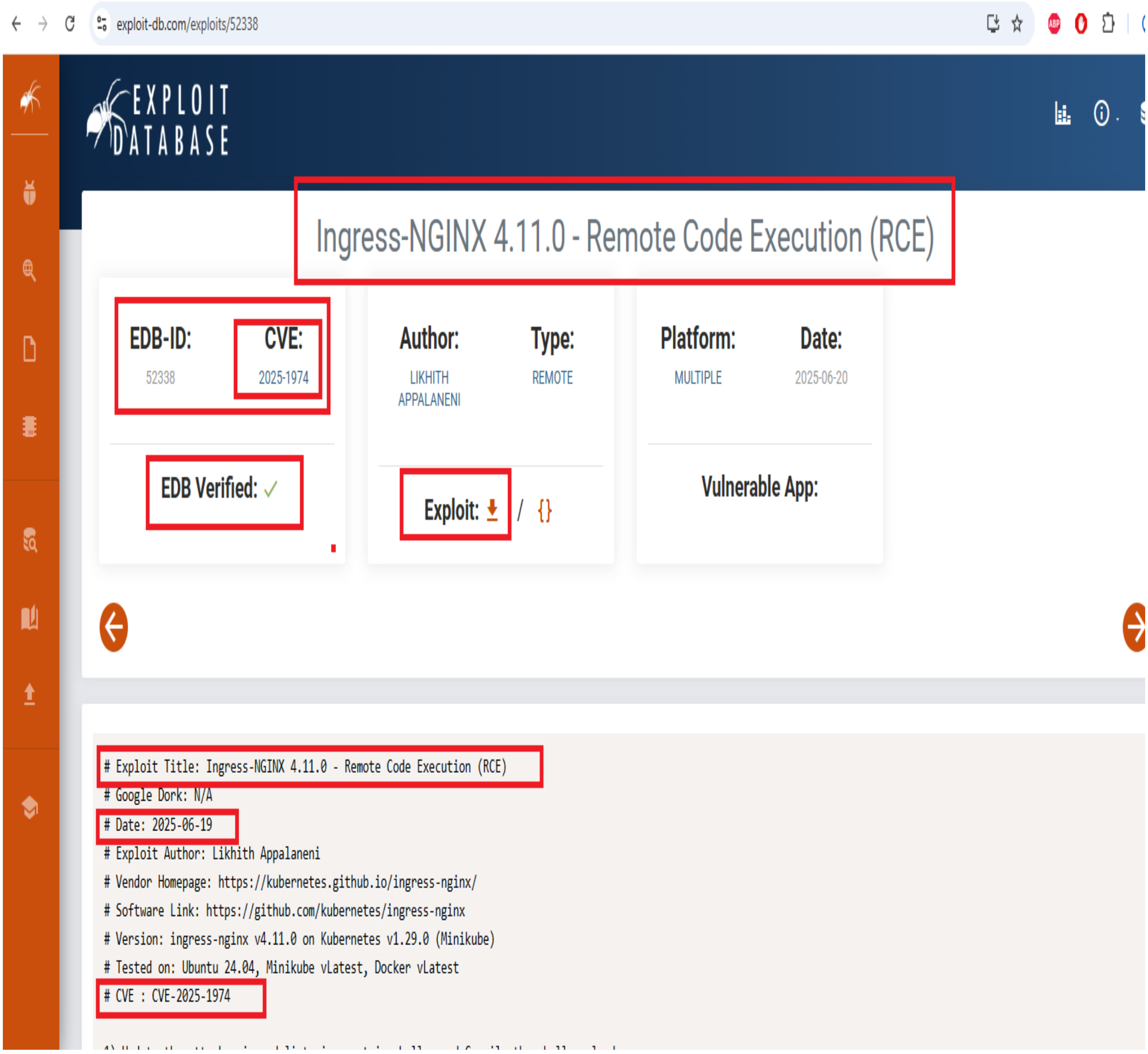
Critical vulnerabilities

ID	Alternative ID	Exploitation	CVSS	Vendor	Changed
EUVD-2025-35061	CVE-2025-10678	Not available	● v4.0 9.3	NetBird VPN	4 hours ago
NetBird VPN does not remove the default password of an admin account					
EUVD-2025-34911	CVE-2025-56218	● 0.02%	● v3.1 9.8	n/a	4 hours ago
An arbitrary file upload vulnerability in SigningHub v8.6.8 allows attackers to execute arbitrary code via uploading a crafted PDF file.					
EUVD-2025-34912	CVE-2025-56316	● 0.04%	● v3.1 9.8	n/a	4 hours ago
A SQL injection vulnerability in the content_title parameter of the /cms/content/list endpoint in MCMS 5.5.0 allows remote attackers to execute arbitrary SQL queries via unsanitized input in the FreeMarker template rendering.					
EUVD-2025-34973	CVE-2025-11391	● 0.13%	● v3.1 9.8	themeisle	6 hours ago
The PPOM – Product Addons & Custom Fields for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the image cropper functionality in all versions up to, and including, 33.0.15. This makes it possible for.					

More critical vulnerabilitie

Fig. 4. Vulnerability database of ENISA

Exploit Database (Exploit-DB) is a practical, community-maintained repository specializing in exploit code and proof-of-concept demonstrations [5]. Unlike theoretical databases, it contains real exploit scripts and tools that can demonstrate how specific vulnerabilities can be used in attacks. For penetration testers, researchers, and red teams, it is an essential source for validating vulnerabilities. Each entry usually links to a CVE identifier, providing clear context and traceability. The platform’s community-driven nature ensures that it remains frequently updated [5], making it a trusted reference for both offensive and defensive cybersecurity work. For defenders, it provides a window into attacker methodologies, helping to test detection and prevention mechanisms. Fig. 5 shows the exploit with remote code execution on Ingress-NGINX 4.11.0.



Ingress-NGINX 4.11.0 - Remote Code Execution (RCE)

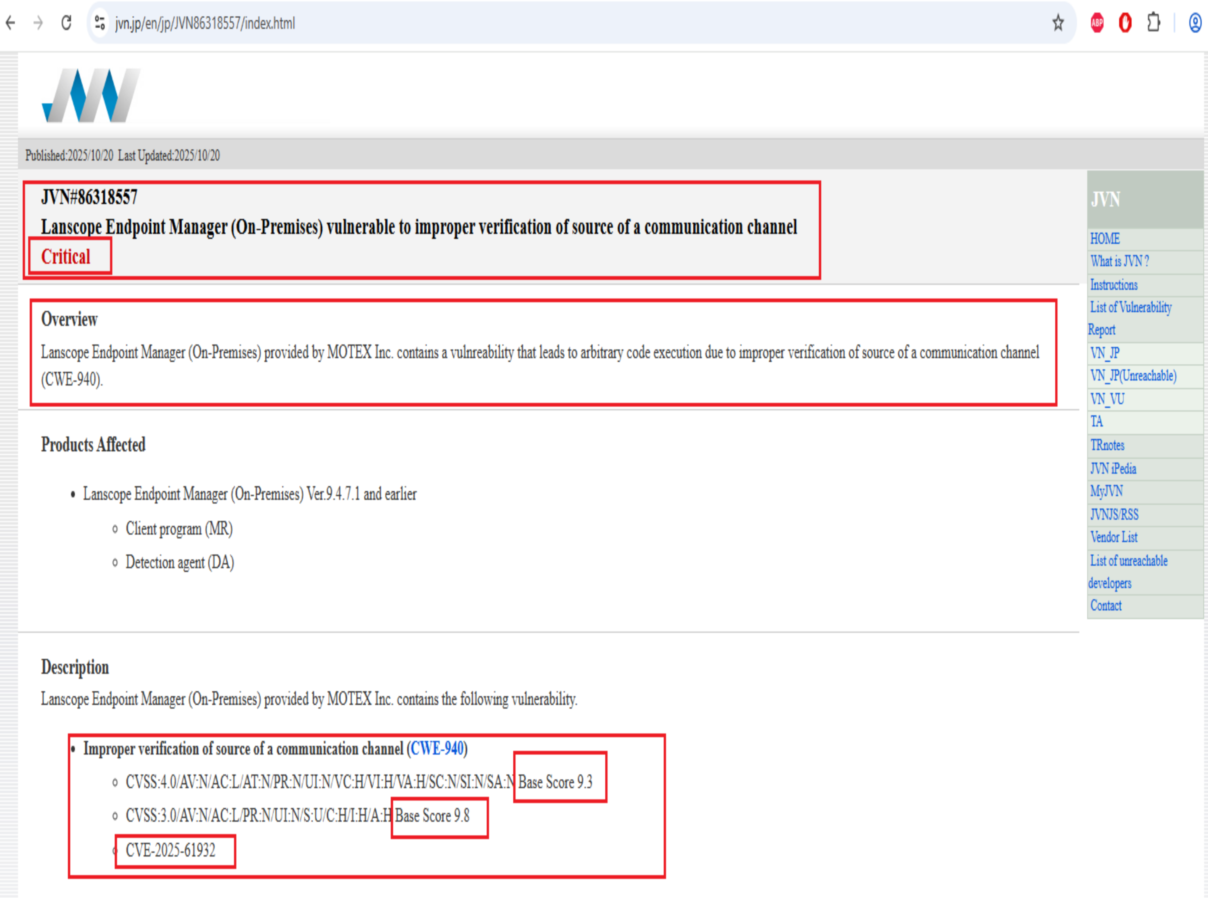
EDB-ID: 52338
CVE: 2025-1974
Author: LIKHITH APPALANENI
Type: REMOTE
Platform: MULTIPLE
Date: 2025-06-20
EDB Verified: ✓
Exploit: / {}
Vulnerable App:

```
# Exploit Title: Ingress-NGINX 4.11.0 - Remote Code Execution (RCE)
# Google Dork: N/A
# Date: 2025-06-19
# Exploit Author: Likhith Appalaneni
# Vendor Homepage: https://kubernetes.github.io/ingress-nginx/
# Software Link: https://github.com/kubernetes/ingress-nginx
# Version: ingress-nginx v4.11.0 on Kubernetes v1.29.0 (Minikube)
# Tested on: Ubuntu 24.04, Minikube vLatest, Docker vLatest
# CVE : CVE-2025-1974
```

Fig. 5. Exploit vulnerability database

Japan Vulnerability Notes (JVN) is a national portal maintained by JPCERT/CC and the Information-Technology Promotion Agency (IPA). Its main function is to localize and analyze global vulnerability data for the Japanese market [8,17]. JVN translates advisories and adds region-specific context, such as how vulnerabilities affect software commonly used in Japan. This approach ensures that local organizations receive timely and understandable security updates. As a result, JVN plays a crucial role in strengthening Japan's cybersecurity ecosystem by bridging global disclosures with domestic awareness [8,17].

The MITRE Corporation acts as a central coordinator in the vulnerability management ecosystem [6,14]. As a non-profit organization, MITRE operates several foundational frameworks, including CVE and CWE, and supports community collaboration across governments, vendors, and researchers [6,14]. Fig. 6 shows another critical found vulnerability with CVSS base score of 9.3 points.



Published:2025/10/20 Last Updated:2025/10/20

JVN#86318557

Lanscope Endpoint Manager (On-Premises) vulnerable to improper verification of source of a communication channel

Critical

Overview

Lanscope Endpoint Manager (On-Premises) provided by MOTEX Inc. contains a vulnreability that leads to arbitrary code execution due to improper verification of source of a communication channel (CWE-940).

Products Affected

- Lanscope Endpoint Manager (On-Premises) Ver.9.4.7.1 and earlier
  - Client program (MR)
  - Detection agent (DA)

Description

Lanscope Endpoint Manager (On-Premises) provided by MOTEX Inc. contains the following vulnerability.

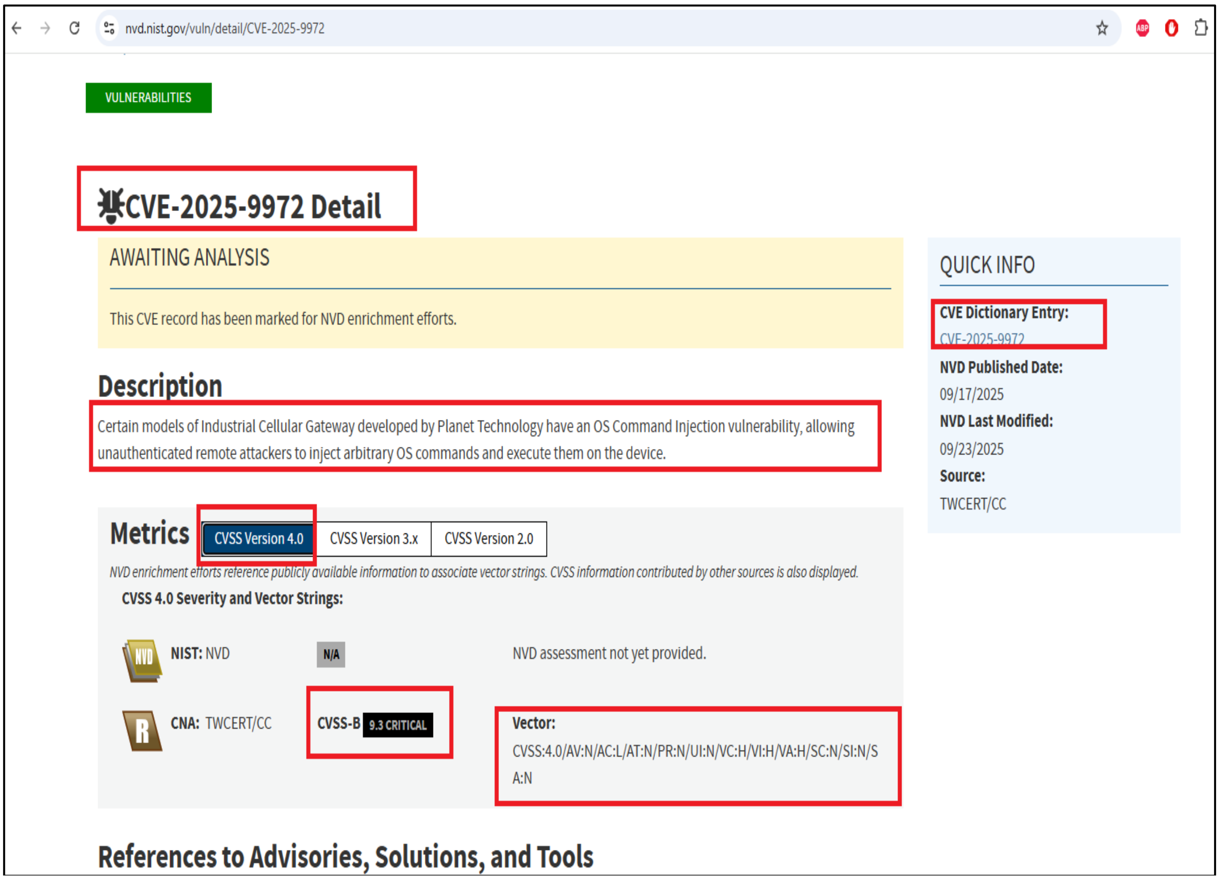
- **Improper verification of source of a communication channel (CWE-940)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score 9.3
  - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score 9.8
  - CVE-2025-61932

Fig. 6. JVN vulnerability database

Its mission extends beyond maintenance and in this context it conducts research, develops new methodologies, and advances standards that underpin global cybersecurity operations. MITRE's neutral and open approach promotes trust, ensuring that its frameworks are widely adopted across both public and private sectors [6,14].

The National Vulnerability Database (NVD) serves as the official U.S. government repository built upon the CVE list. Managed by the National Institute of Standards and Technology (NIST), it extends basic CVE records with comprehensive analysis, including CVSS scores and CWE categorizations

[7,10,12]. The NVD also provides metadata on affected products and available remediations. Because of its depth and reliability [7,10,12], it is widely integrated into vulnerability scanners, management tools, and academic research. Analysts rely on its datasets to automate prioritization and reporting workflows. In essence, the NVD transforms CVE identifiers into actionable intelligence, becoming a cornerstone of operational cybersecurity [7,10,12]. Fig. 7 presents the detailed CVE information for the vulnerability with number 2025-9972.



CVE-2025-9972 Detail

AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

Description

Certain models of Industrial Cellular Gateway developed by Planet Technology have an OS Command Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on the device.

Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 4.0 Severity and Vector Strings:

NIST: NVD N/A NVD assessment not yet provided.

CNA: TWCERT/CC CVSS-B 9.3 CRITICAL Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

References to Advisories, Solutions, and Tools

QUICK INFO

CVE Dictionary Entry: CVE-2025-9972

NVD Published Date: 09/17/2025

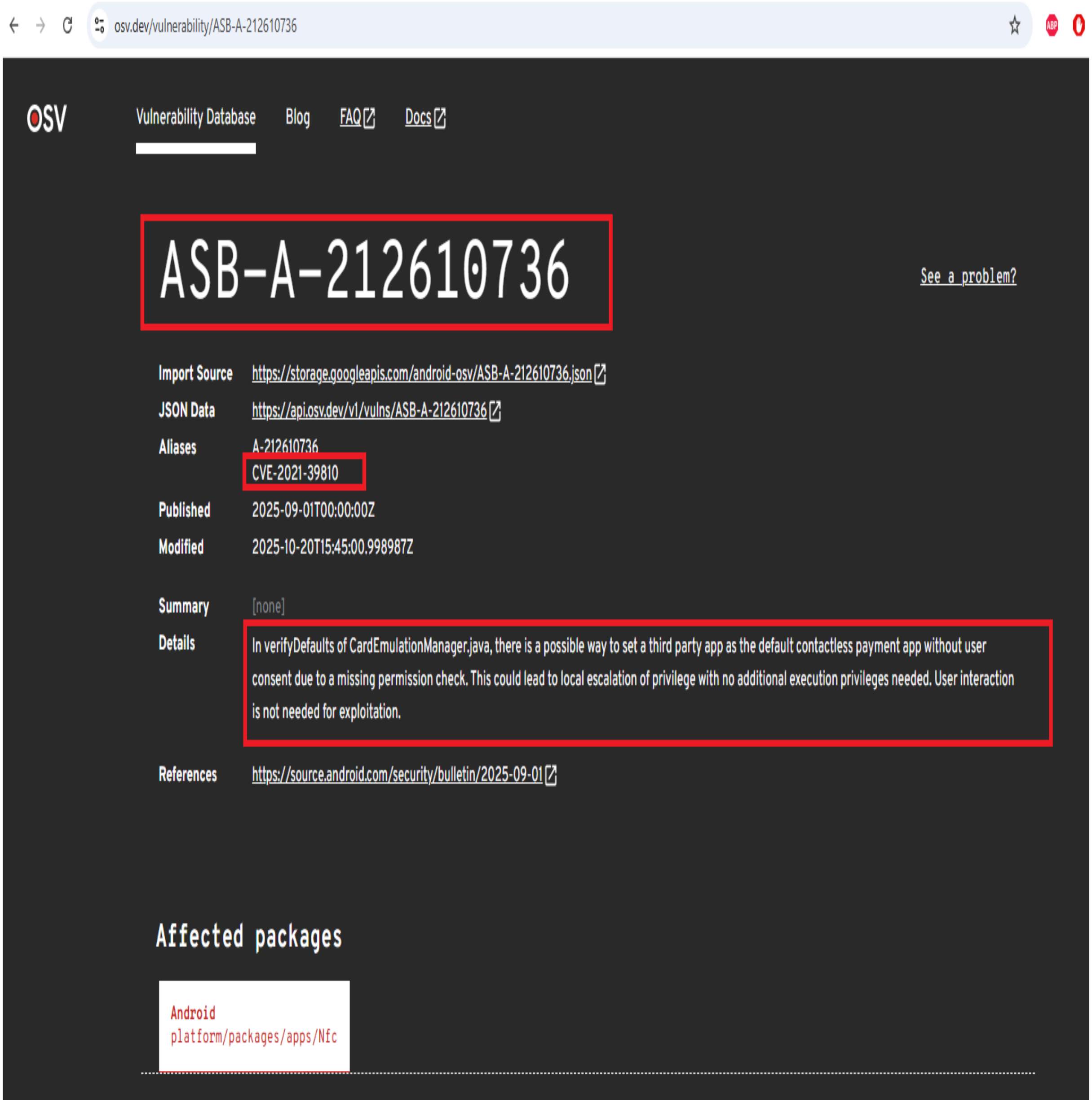
NVD Last Modified: 09/23/2025

Source: TWCERT/CC

Fig. 7. NVD vulnerability database

The Open Source Vulnerability Database (OSVDB) was one of the earliest community-driven repositories documenting software flaws [4,18]. Operating for over a decade, it offered detailed, human-written analyses for each entry and was widely appreciated for its independence and depth. Despite its success, OSVDB was discontinued in 2016 due to financial and operational challenges [4,18]. Its closure left a noticeable gap in the open-source security landscape, underscoring the difficulties of sustaining large-scale volunteer-based initiatives. Still, OSVDB remains an important milestone in the history of vulnerability information sharing [4,18].

The cybersecurity firm Rapid7 operates a proprietary vulnerability intelligence database that integrates tightly with its Metasploit framework [9,19]. The repository emphasizes the practical exploitability of vulnerabilities, including details about exploit availability, weaponization, and real-world attack activity observed by the company’s threat intelligence team. This contextual insight enables organizations to prioritize remediation based on active exploitation trends [9,19]. Because Rapid7 functions both as a security product vendor and a research entity [9,19], its database represents the convergence of commercial intelligence and empirical analysis. Fig. 8 illustrates a vulnerability detected in Android based systems.



ASB-A-212610736

Import Source https://storage.googleapis.com/android-osv/ASB-A-212610736.json

JSON Data https://api.osv.dev/v1/vulns/ASB-A-212610736

Aliases A-212610736
CVE-2021-39810

Published 2025-09-01T00:00:00Z

Modified 2025-10-20T15:45:00.998987Z

Summary [none]

Details In verifyDefaults of CardEmulationManager.java, there is a possible way to set a third party app as the default contactless payment app without user consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

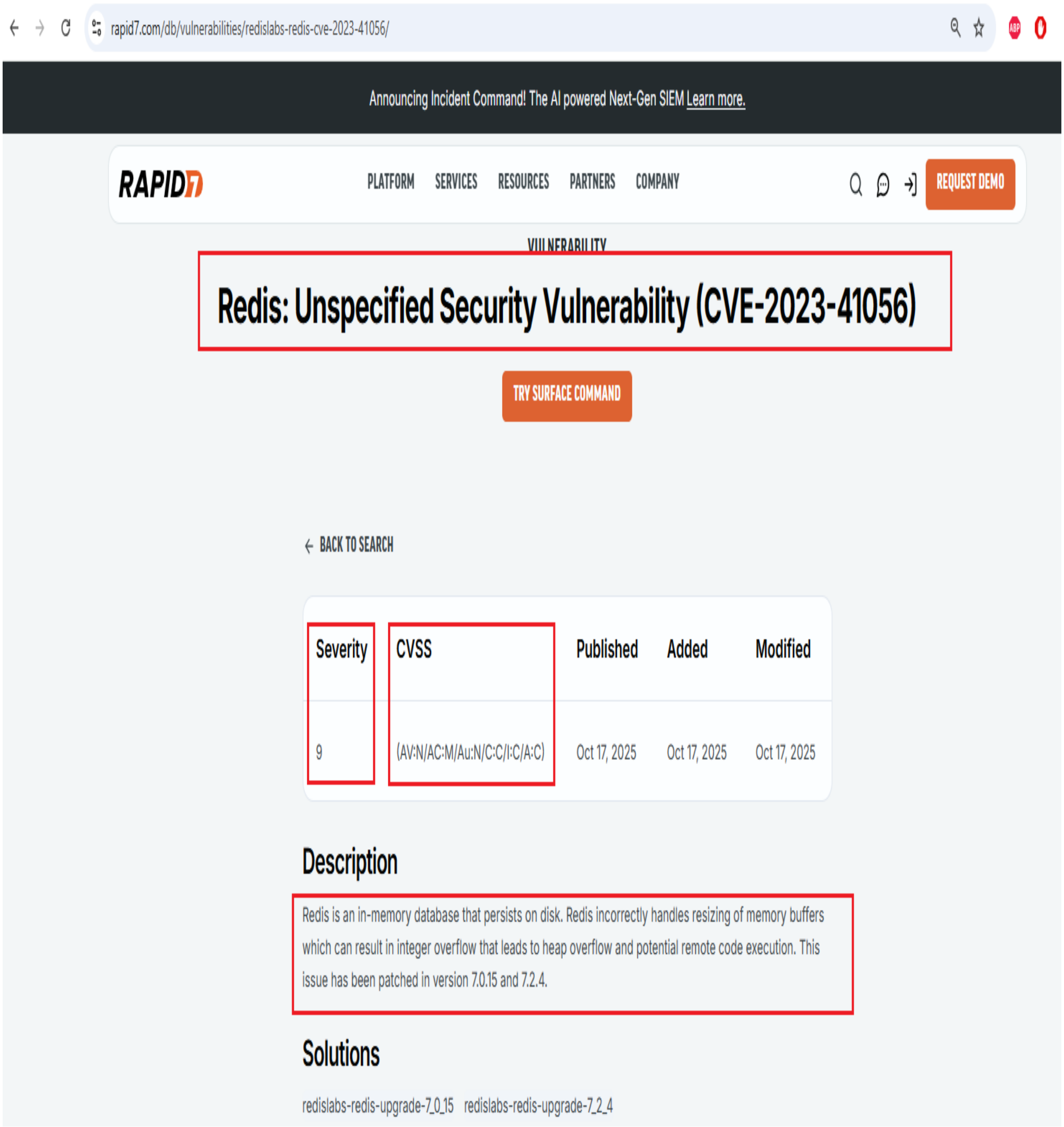
References https://source.android.com/security/bulletin/2025-09-01

Affected packages

Android
platform/packages/apps/Nfc

Fig. 8. OSVDB vulnerability database

The Vulnerability Exploit Database and Aggregation System (VEDAS) represents a research-oriented approach to vulnerability analysis [16]. Its strength lies in aggregating and correlating data from numerous public sources through automation [16]. Using data mining and machine learning, VEDAS identifies trends, predicts the appearance of new exploits, and supports proactive defense strategies. By modeling the lifecycle of vulnerabilities from disclosure to exploit development and it provides predictive insight that helps organizations shorten exposure windows [16]. Such systems illustrate the shift from static documentation toward dynamic, data-driven vulnerability intelligence. Fig. 9 shows unspecified security vulnerability in the database of Redis.


rapid7.com/db/vulnerabilities/redislabs-redis-cve-2023-41056/
Announcing Incident Command! The AI powered Next-Gen SIEM Learn more.
RAPID7
PLATFORM
SERVICES
RESOURCES
PARTNERS
COMPANY
REQUEST DEMO
VULNERABILITY
TRY SURFACE COMMAND
BACK TO SEARCH

Redis: Unspecified Security Vulnerability (CVE-2023-41056)

Severity	CVSS	Published	Added	Modified
9	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	Oct 17, 2025	Oct 17, 2025	Oct 17, 2025

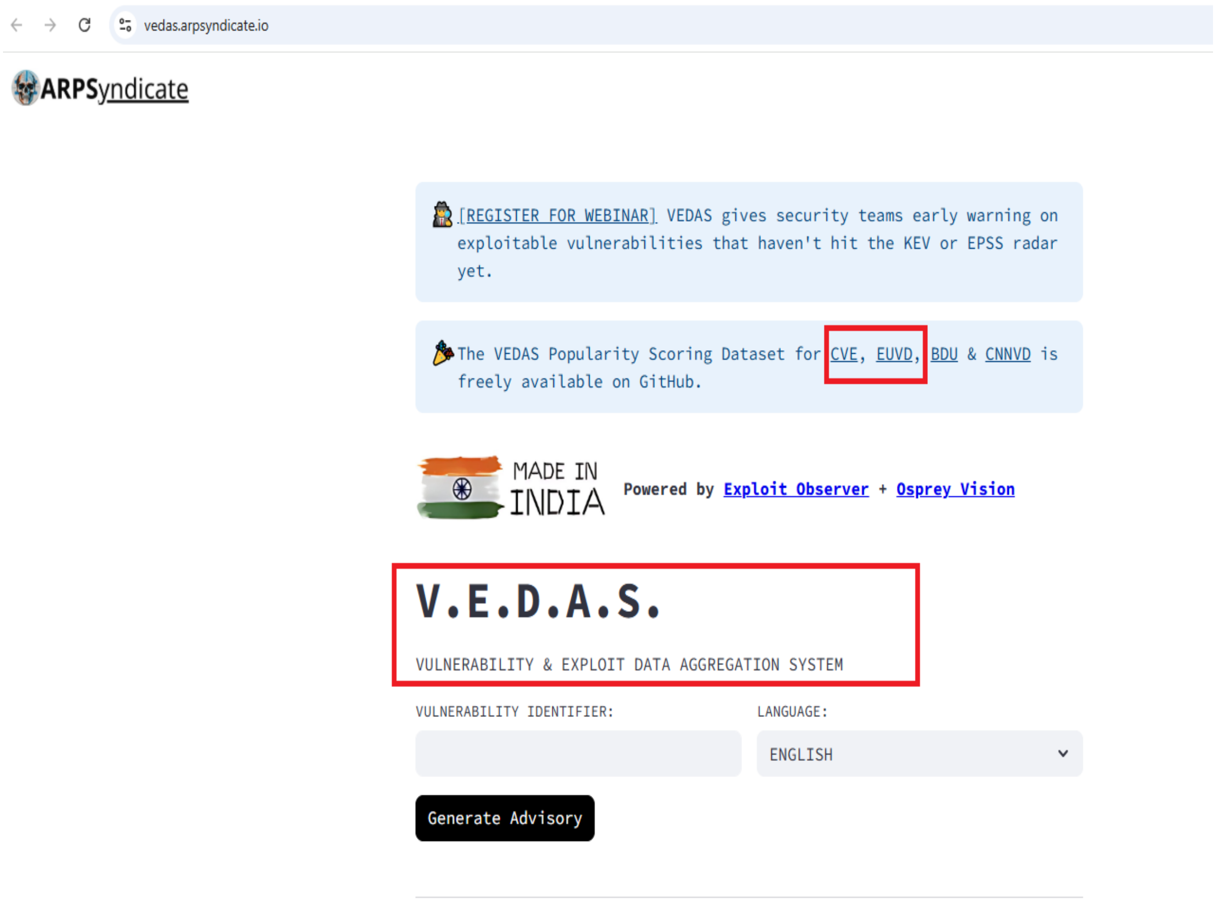
Description

Redis is an in-memory database that persists on disk. Redis incorrectly handles resizing of memory buffers which can result in integer overflow that leads to heap overflow and potential remote code execution. This issue has been patched in version 7.0.15 and 7.2.4.

Solutions

redislabs-redis-upgrade-7_0_15 redislabs-redis-upgrade-7_2_4

Fig. 9. Rapid7 vulnerability database



vedas.arpsyndicate.io

ARPSyndicate

[REGISTER FOR WEBINAR] VEDAS gives security teams early warning on exploitable vulnerabilities that haven't hit the KEV or EPSS radar yet.

The VEDAS Popularity Scoring Dataset for CVE, EUVD, BDU & CNNVD is freely available on GitHub.

MADE IN INDIA

Powered by Exploit Observer + Osprey Vision

V.E.D.A.S.

VULNERABILITY & EXPLOIT DATA AGGREGATION SYSTEM

VULNERABILITY IDENTIFIER:

LANGUAGE: ENGLISH

Generate Advisory

Fig. 10. VEDAS vulnerability database

3. Conclusion

This comparative analysis highlights how complex and interconnected today's vulnerability management ecosystem has become. The progression from simple standardized identifiers in CVE to the detailed and contextualized records of the NVD illustrates the evolution from basic cataloging toward actionable intelligence. Throughout this study, it became clear that while CVSS provides an essential, if sometimes imperfect, metric for prioritizing risks, CWE adds a valuable structural perspective by focusing on the underlying causes of vulnerabilities rather than just their manifestations.

Specialized repositories such as Exploit-DB [5] and Rapid7-DB [9] add practical insight by demonstrating how theoretical weaknesses translate into real-world exploitation, thus bridging the gap between analytical assessment and operational threat. At the same time, international platforms like Japan Vulnerability Notes emphasize [8,17] the importance of adapting global vulnerability data to local languages, technologies, and regulatory settings. The historical contribution of community-led projects such as OSVDB also serves as a reminder of how challenging it is to sustain independent and comprehensive databases over time.

In practice, none of these systems function effectively in isolation. Their collective value comes from the way they complement and enrich one another through integration and shared standards. A mature cybersecurity strategy therefore relies on the combined strength of these systems rather than any single repository. Looking forward, the continued development of data-sharing frameworks, interoperability standards, and collaborative research will be crucial for transforming vulnerability data into proactive, context-aware defense capabilities.

Acknowledgments

This scientific article under project number RD-08-124/07.02.2025 „Renewing the research environment for collecting empirical data in measurement processes“, at Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences is funded.

References:

[1] Anderson, K., "The CVE Ecosystem: A Decade of Standardizing Vulnerability Identification," Journal of Cybersecurity Advances, vol. 5, no. 2, pp. 45-60, 2021, ISSN 1234-5678, DOI: 10.1000/cyber.2021.12345.

[2] Brown, L., & Chen, M., "Beyond the Score: A Critical Analysis of CVSS Limitations in Modern Threat Landscapes," in Proc. International Conference on Security and Privacy (ICSP), IEEE, 2019, pp. 234-248, ISBN 978-1-1234-5678-9, DOI: 10.1000/icsp.2019.56789.

[3] Davis, R., "CWE as a Framework for Secure Software Development Lifecycles," IEEE Transactions on Software Engineering, vol. 48, no. 4, pp. 112-125, 2020, ISSN 0098-5589, DOI: 10.1109/TSE.2020.9876543.

[4] Fischer, S., "A Forensic Analysis of the OSVDB: Lessons from a Community-Driven Project," Digital Investigation Journal, vol. 15, no. 1, pp. 78-91, 2018, ISSN 1742-2876, DOI: 10.1016/j.diin.2018.01.005.

[5] Garcia, P., "Exploit-DB and the Democratization of Offensive Security Tooling," Computers & Security Review, vol. 32, no. 3, pp. 201-215, 2017, ISSN 0167-4048, DOI: 10.1016/j.cose.2017.03.008.

[6] Harris, T., "The Role of MITRE in Shaping Global Cybersecurity Frameworks," Strategic Security Analysis, vol. 12, no. 4, pp. 33-47, 2022, ISSN 2345-6789.

[7] Johnson, A., & Lee, S., "A Comparative Study of National Vulnerability Databases: NVD and the Emerging EUVD," in Proc. World Conference on Information Security (WCIS), ACM, 2021, pp. 501-515, ISBN 978-1-9876-5432-1, DOI: 10.1145/1234567.1234568.

[8] Kato, Y., "Japan Vulnerability Notes (JVN): Localizing Global Threat Intelligence," Journal of Regional Cybersecurity, vol. 4, no. 1, pp. 22-35, 2019, ISSN 2567-1234.

[9] Martinez, D., "Integrating RAPID7-DB for Enhanced Threat Intelligence in SIEM Platforms," in Proc. Conference on Data and Application Security (CODASPY), ACM, 2020, pp. 145-156, ISBN 978-1-1357-9246-0, DOI: 10.1145/1234567.1234569.

[10] Miller, B., "The National Vulnerability Database (NVD): An Analysis of its Enrichment Process and Impact," Government Information Quarterly, vol. 38, no. 2, 2021, ISSN 0740-624X, DOI: 10.1016/j.giq.2021.101567.

[11] Nielsen, J., "Vulnerability Assessment and the Critical Role of CVE Identifiers," in Cybersecurity Fundamentals, 2nd ed., TechPress, 2018, pp. 155-170, ISBN 978-1-2345-6789-0.

[12] O'Malley, C., "From CVE to Patch: A Practical Guide Using NVD and Exploit-DB," SysAdmin Today, vol. 25, no. 6, pp. 44-50, 2019, ISSN 0895-6758.

[13] Patel, R., "A Quantitative Evaluation of CVSS Base Metrics for Vulnerability Prioritization," ACM Computing Surveys, vol. 55, no. 8, pp. 1-35, 2022, ISSN 0360-0300, DOI: 10.1145/1234567.1234567.

[14] Roberts, E., "The Evolution of MITRE ATT&CK and CWE: A Synergistic Approach," Journal of Threat Intelligence, vol. 7, no. 1, pp. 88-102, 2023, ISSN 2567-4567.

[15] Simeonova, I., Metodieva, TS., Model for administrative security management in a municipality, Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 26, Shumen, 2024, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 93-105, DOI: https://doi.org/10.46687/jsar.v26i1.397.

[16] Smith, J., "Automating Vulnerability Intelligence: A Deep Dive into the VEDAS Framework," in Proc. International Workshop on Security and Privacy Analytics (IWSPA), Springer, 2016, pp. 112-126, ISBN 978-3-031-23456-7, DOI: 10.1000/182-3-031-23456-7_8.

[17] Tanaka, H., "A Survey of Vulnerability Disclosure in Japan: The Role of JVN and JPCERT/CC," Pacific Rim Cybersecurity Review, vol. 9, no. 2, pp. 15-29, 2020, ISSN 1897-1234.

[18] Thompson, G., "The Legacy and Impact of OSVDB on Open Source Security," IEEE Security & Privacy Magazine, vol. 16, no. 5, pp. 70-75, 2018, ISSN 1540-7993, DOI: 10.1109/MSEC.2018.2855123.

[19] Wagner, M., "Operationalizing Threat Data: A Case Study of Rapid7-DB and Metasploit," SANS Reading Room Whitepaper, 2019, [Online] Available: https://www.sans.org/reading-room/whitepapers/.

[20] Williams, F., "Building a Proactive Defense with CWE-Based Code Analysis," in Secure Software Design: Principles and Practices, Academic Press, 2017, pp. 99-120, ISBN 978-0-1234-5678-1.

[21] Zhang, W., "A Federated Model for a European Vulnerability Database (EUVD): Challenges and Opportunities," in Proc. European Symposium on Security and Privacy (EuroS&P) Workshops, IEEE, 2022, pp. 301-310, ISSN 2768-0657, DOI: 10.1109/EuroSPW.2022.00045.