Beyond the CVSS: Rethinking the Contextualisation of CVEs in a Connected World

Myriam Ouraou
Thales Digital Factory, Paris, France
ESILV, Paris, France

myriam.ouraou@edu.devinci.fr

Abstract: In the context of globalized information technology, managing the growing number of Common Vulnerability Exposures (CVE) has become one of the most complex challenges for security teams. CVEs affect everyone: whether you are Microsoft Corporation, a national government, or an ordinary global citizen, no one is immune. The burden on cybersecurity entities is now heavier than ever. The more diverse assets a system holds, the broader its monitoring scope must be. Therefore, to avoid overwhelming operational and security teams, it is crucial to adapt the contextualization of CVEs to address emerging risks proactively and effectively. This involves not only analysing the technical characteristics of vulnerabilities but also considering contextual factors, and the dynamics of the global threat landscape. Relying solely on the CVSS Score is no longer sufficient; the rise of new indicators offers a fresh perspective on how security teams contextualize vulnerabilities. For effective vulnerability management within an environment, it is essential to first assess its level of maturity: from the most basic process, which allows for simple identification of vulnerabilities and asset patching, to the most advanced level, which incorporates the integration of business and IT impacts, the clear identification of priority threat vectors, and a continuous remediation process. However, since the beginning of 2024, the vulnerability management process for entities has been significantly disrupted by the absence of analysis from the NVD (National Vulnerability Database) of the NIST (National Institute of Standards and Technology). As the NVD is the primary source for publishing CVEs, this lack of information has hindered processes, leaving organisations with only partial analysis based on vendor assessments, which are often insufficient and differ from those of the NVD. In this paper, we intend to examine the various levels of maturity that a vulnerability management process must go through during its existence, the definition of the different indicators that characterize CVEs and we will reflect on the dependence of the NVD in the processes.

Keywords: Vulnerability, CVE, CVSS, EPSS, Contextualisation, Management

1. Introduction

Information technology is the mainstay of our modern societies, affecting every aspect of daily life. From trading floors, through our social interactions, to national votes, our world is becoming ultra-connected. However, despite this growing dependence on digital technologies, cybersecurity is often relegated to the background, overshadowed by business priorities aimed at cutting costs and speeding up the development of new functionalities.

Nevertheless, faced with the explosion in cyber threats and increasingly sophisticated attacks, a great deal of effort is being made to strengthen the security of platforms. In a globalised world, systems are interconnected. A flaw in one is an open door in another. Security incidents have an impact not just on a system, but also on an organisation's reputation. Vulnerability management is therefore becoming a central issue in cyber intelligence activities because the slightest flaw can have disastrous consequences for an organisation. In 1999, the Common Vulnerabilities and Exposures (CVE) were created by the MITRE Corporation, a non-profit organisation in the United States. They were created in response to a growing need to standardise the way computer security vulnerabilities were identified and catalogued. The main purpose of CVEs is to provide a common public nomenclature for referencing vulnerabilities, thereby easing the communication, assessment, and management of security risks across different industries. Each CVE is given a unique identifier of the form CVE-YEAR-XXXXX, which allows companies, developers, and security researchers to refer to a specific vulnerability in a clear and consistent way.

It was against this backdrop that the Common Vulnerability Scoring System (CVSS) was created. It assigns a numerical score between 0.1 and 10. Since its start, it has evolved through several phases - from version v2.0 to the recent version v4.0 - each seeking to better reflect the criticality of vulnerabilities. However, relying solely on the CVSS to assess and prioritise vulnerabilities is now showing its limitations. Although it provides a useful technical score, the CVSS does not take sufficient account of the specific realities of organisations, such as the operational impact, remediation costs or the management of priorities based on available resources.

What is more, the volume of CVEs published has exploded in recent years, putting considerable pressure on security teams. In 2023 alone, 30,000 CVEs has been identified, compared with 20,000 in 2020. Exhaustive and reactive remediation of vulnerabilities is becoming impossible for many organisations. It is therefore crucial to

know where to place the cursor between security and business aims. This article will first look at how to set up a mature process, the discovery of various tools for contextualising CVEs and then discuss the quest for independence in the analyses. This reflection is the fruit of a long process of industrialisation of a vulnerability management process within a cloud environment.

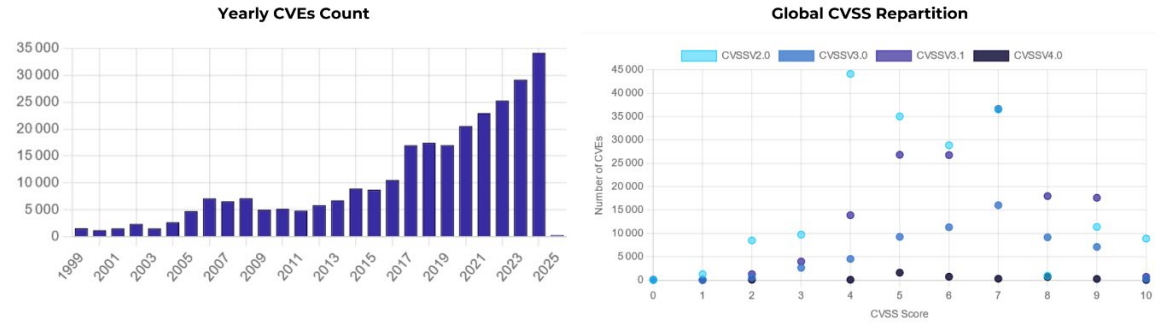

Figure 1: Number of CVEs over the years (OpenCVE)

2. Process Maturity

2.1 Identification of Assets and Vulnerabilities

There are four key stages in vulnerability management: identification, analysis, prioritisation, and remediation. Of these, the identification phase is of crucial importance, as it decides the accuracy and relevance of the entire process. Its main aim is to establish an exhaustive map of the perimeter to which the vulnerability management process applies, including a detailed inventory of hardware and software assets within the environment. The more accurate this inventory is, the more dependable and targeted the identification of vulnerabilities (CVEs) will be.

As a reminder, a CVE is a unique identifier assigned to a security vulnerability. It is generally accompanied by several key elements: a CVSS (Common Vulnerability Scoring System) score, which measures the severity of the vulnerability; a CPE (Common Platform Enumeration), which specifies the products and versions concerned; a CWE (Common Weakness Enumeration), which describes the nature of the vulnerability; and a vector chain, which details the technical characteristics of the exploitability and impact. Once the perimeter has been mapped, vulnerabilities can be identified based on this. This mapping must be regularly updated to reflect any addition, modification, or deletion of assets within the information system. As vulnerabilities are version-specific, it is essential to have precise information on the versions in place. In cases where this information is not at once available, security teams must be able to find it quickly, as incomplete data hinders the ability to assess vulnerabilities and apply necessary patches.

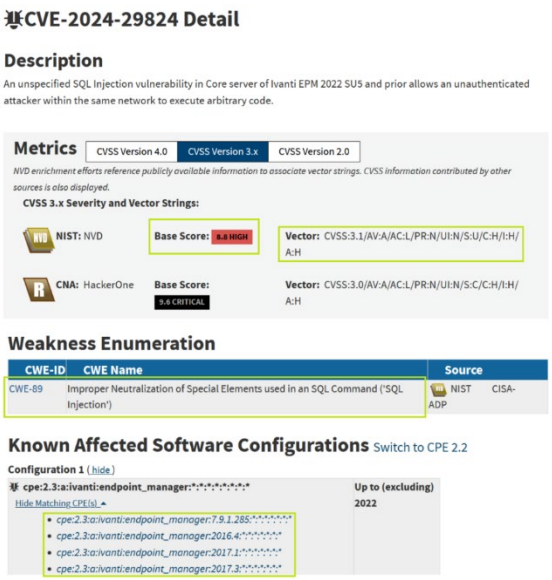

Figure 2: CVE presentation (NVD)

2.2 Analysis

The analysis phase of a vulnerability allows us to understand how it can be exploited and in what context it represents a threat to the organisation. This includes examining the conditions required for exploitation and the interactions between the vulnerability and other system components to better understand the scope of its potential effects. Another aspect not to be overlooked is the search for existing exploits. By analysing code or scripts that are already available with your technical teams, you can assess how dangerous they really are and understand the methods that attackers might use thanks to their expertise.

For example, the CVE in Figure 2 is an SQL injection in one of Ivanti's products. It is characterised as having a significant impact on all the CIA pillars and is also being actively exploited. It should also be noted that the Attack Vector is of the “Adjacent” type, which means that the attacker must be on the same network as the target or in an environment where direct communication between the attacker and the target is possible.

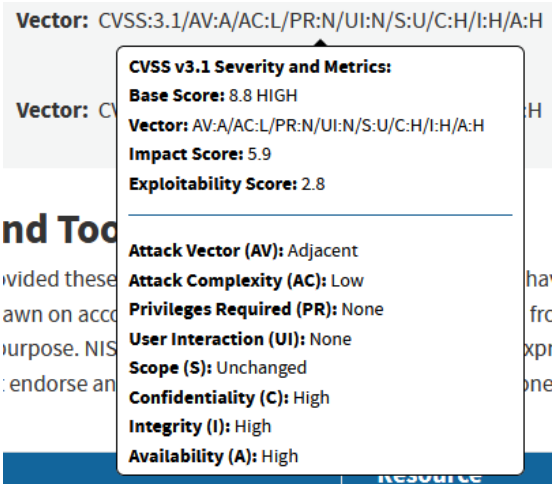

Figure 3: CVE-2024-29824's Vector String (NVD)

2.3 Measuring Impact and Prioritising

Once the vulnerabilities have been analysed, they need to be contextualised and their impact within the environment defined. Each vulnerability will not behave in the same way in two different systems. It is therefore necessary to reassess the risk associated with a vulnerability. Risk is the probability that a threat will exploit a vulnerability, resulting in negative impacts on an information system. The key point at this stage is therefore to assess the negative impact on the perimeter. Two types of impact need to be distinguished but correlated: business impact and operational impact.

The business impact of a vulnerability refers to the consequences that exploiting this vulnerability can have on an organisation's strategic, financial, and commercial aims. This directly affects an organisation's profitability, reputation, and market positioning. Operational impacts concern the direct effects on the organisation's day-to-day activities, internal processes, and technical infrastructure. They affect the way teams and systems run on a day-to-day basis.

Based on the analyses conducted in the earlier stage, it is necessary to define the probability of the vulnerability being exploited within the system. Particular attention should be paid to the grouping of CVEs on the same asset and to the links between software dependencies to reduce the risk of a cascade attack in complex, interconnected environments. However, not all vulnerabilities can be corrected at once, especially when our perimeter has many dependencies and interconnections. It is therefore essential to decide which ones require urgent action to optimise resources and minimise risks and costs. But prioritising vulnerabilities is subject to several constraints: the criticality of the assets concerned, the exposure of the vulnerable assets, the dependencies of vulnerable assets, the external pressure (e.g. zero-day), the available resources, the maintenance schedules.

These constraints may lead to a reassessment of the risk, the remediation period but also reduce the scope of grouped CVEs. Nevertheless, due diligence must be exercised: prioritising vulnerabilities is a balancing act between security and business requirements, where it is imperative to choose judiciously the actions to be taken according to the resources and risk involved.

2.4 Continuous Remediation

Continuous remediation is based on an initiative-taking strategy, where vulnerability management is not limited to reactive actions in the face of incidents, but is part of a regular cycle of improvement and maintenance. This approach has two components: permanent remediation and one-off remediation.

Permanent remediation is based on predefined maintenance schedules, which concern updates to operating systems, packages and the software used. These scheduled updates address discovered vulnerabilities and keep the information system up to date, reducing exposure windows to threats. One-off remediation becomes necessary when a vulnerability is identified and prioritised. Often associated with strategic or externally exposed assets, these require an immediate response to reduce the risk of compromise.

One of the biggest challenges for organisations is keeping their major assets up to date. These infrastructures are often neglected because of the complexity of major updates and the fear of disrupting production environments, especially when there is a long-time lag between two versions. This situation creates a twofold risk: firstly, the longer the patching time, the longer the vulnerable asset stays exposed to threats. Secondly, teams often must spend more time resolving compatibility issues than implementing the patches themselves, thereby delaying the securing of systems.

The result is a prolonged period of vulnerability, often unacceptable in critical environments. The remediation schedule must therefore differentiate between critical assets in production and those in test or development environments. This flexibility ensures greatest management of resources without sacrificing security.

3. Prioritisation Tools

3.1 CVSS: A Constantly Evolving Indicator

The CVSS is a vulnerability scoring framework introduced in 2005 by the Forum of Incident Response and Security Teams (FIRST). Its main aim is to provide an open standard for classifying vulnerabilities according to their severity to help organisations prioritise their remediation efforts. Since its start, CVSS has evolved to better reflect the increasing complexity of modern IT environments and security threats.

The first version of the CVSS was designed to standardise the way vulnerabilities are assessed and rated across different industries. CVSS v1 proposed an assessment based on three groups of scores: Impact, Exploitability, Scope.

In 2007, the second version was introduced: a revision that brought greater finesse to vulnerability assessment. CVSS v2.0 introduced adjustments to the scoring model to make the framework more usable and intuitive. With the emergence of modern technologies and more complex attack models, CVSS v3.0, published in 2015, made improvements to make the system more relevant to modern challenges. It introduced new concepts: Extended Scope, Privileges required, Complexity of the attack, User interaction.

In 2019, CVSS v3.1 was released to provide clarifications without radically changing the scoring framework. The main purpose of this update was to improve the documentation and refine the definition of certain metrics to resolve ambiguities met in v3.0. It also reinforced the use of the Vector String, which provides a textual representation of the full notation of a vulnerability.

CVSS v4.0 was introduced only recently, in November 2023, in response to persistent criticism and to adapt to new cybersecurity challenges. It introduces significant changes compared with earlier versions. One of the main new features is the addition of new metrics, such as Exploit Maturity, which assesses the degree to which exploits are developed and used, and Automated Targeting, which measures the ability of an attack to be automated and propagate without human interaction. These metrics provide a more accurate assessment of how dangerous vulnerabilities are. In addition, CVSS v4.0 includes the ability to further customise scores according to specific environments, as well as better recognition of interconnected vulnerabilities affecting the same asset. These new features make risk assessment more realistic and adapted to modern infrastructures, particularly cloud and hybrid environments.

However, since its publication, the CVSS v4.0 standard has not been widely used, and the v3.1 standard is still in use today. This phenomenon already occurred when version v2.0 was upgraded to v3.x. Few years ago, on the APIs (Application Programming Interface) of certain publishers, many scores were still published according to version v2.0 and did not offer the possibility of recovering the score in version v3.x. We are therefore left with a model that is adapted to today's challenges, but which is still largely absent from our evaluations, making it difficult to adopt and revise CVE analysis methods. There are reasons for the slow adoption of v4.0: Firstly,

integrating the standard into vulnerability management tools and security databases takes time and often requires complex model updates. In addition, some companies are reluctant to change their vulnerability management processes because of the cost and effort associated with this transition.

As CVSS evolves, it becomes clear that the specific context of each organisation is essential for accurate and relevant vulnerability scanning. Although CVSS v4.0 introduces significant improvements, these developments do not replace the need to contextualise results. A CVSS score, even if calculated using the latest metrics, is not sufficient on its own to determine the real impact of a vulnerability on a given environment.

3.2 EPSS: A More Reliable Indicator?

The EPSS (Exploit Prediction Scoring System) is a statistical model designed to assess the likelihood of a computer vulnerability being exploited in the wild within its first 30 days of publication. The FIRST community developed it to help organisations prioritise their remediation efforts based on the risk of actual exploitation. It uses a variety of data sources, such as security incident reports, vulnerability descriptions and exploit information available in public databases. It then assigns a score, between 0 and 1, to each vulnerability, showing the likelihood of it being actively exploited by cybercriminals.

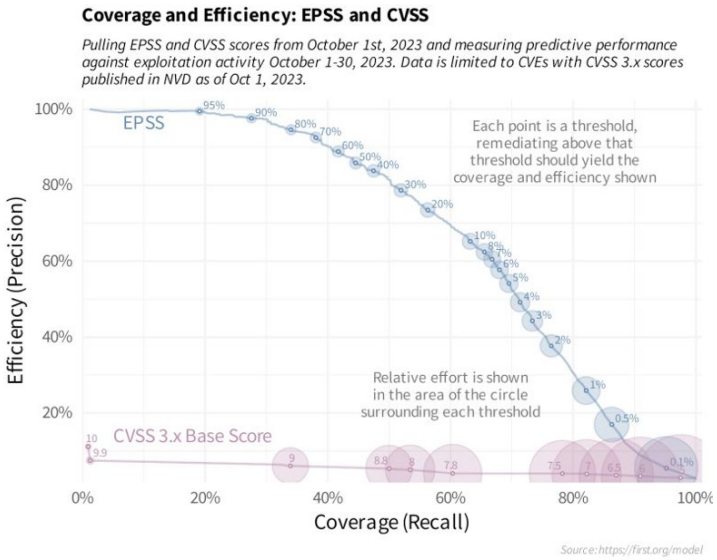

Figure 4: Coverage and efficiency of CVSS and EPSS (FIRST)

Efficiency measures how effectively resources have been used by calculating the percentage of prioritised vulnerabilities that have been exploited. Coverage is the percentage of exploited vulnerabilities that have been prioritised.

Here, we notice that the CVSS is quite inefficient, whether the CVE coverage is small or large. In contrast, the EPSS shows that the smaller the coverage, the higher the efficiency, meaning that remediation efforts are reduced. Typically, let us compare two types of prioritisations:

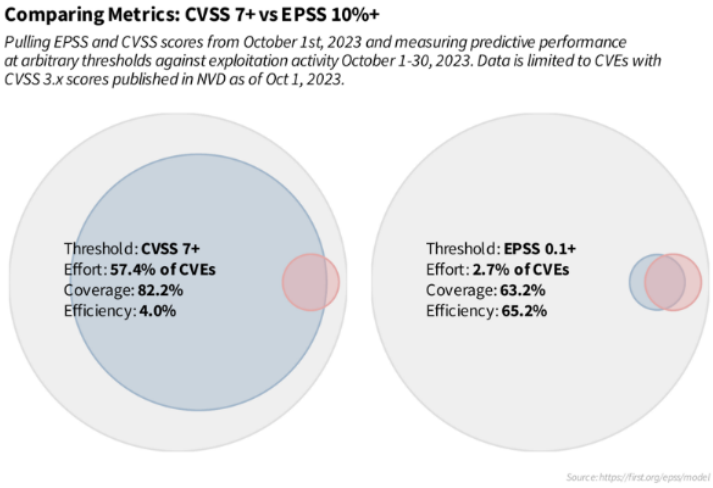

Figure 5: Comparison of CVSS and EPSS metrics (FIRST)

On the left of the Figure 5, prioritisation is based on a CVSS threshold of 7 or higher, and on the right, based on an EPSS threshold of 10% or higher. The blue circles represent the number of CVEs that meet these thresholds, while the red circles represent the number of CVEs that meet the thresholds and have been exploited in the wild. There is a noticeable difference in the size of the blue circles, giving us an idea of the effort needed for each prioritisation strategy. Unlike the CVSS threshold, the EPSS threshold of 10% shows that the effort is significantly lower because there are far fewer vulnerabilities to prioritise, reducing the time and resources needed. Its efficiency is also much higher, as organisations can focus on vulnerabilities that would have the most impact if not addressed first.

One of the main challenges with EPSS lies in the quality and diversity of the data used. Although the model is based on a wide range of sources, it heavily relies on the availability and accuracy of this data. Information about actual attacks is not always accessible, as many companies do not publicly share their security incidents or may underestimate certain minor incidents. Moreover, EPSS is designed for short-term prioritisation. However, a vulnerability could be exploited beyond this window. Therefore, organisations must ensure they do not underestimate the risks associated with vulnerabilities that could become targets overall.

3.3 SSVC: A Prioritisation-Focused Indicator

The SSVC (Stakeholder-Specific Vulnerability Categorization) is a framework developed jointly by Carnegie Mellon University and the Cybersecurity Infrastructure Security Agency (CISA). It was created to address the need for a more contextualised approach to vulnerability management. Unlike CVSS, which calculates a score primarily based on the technical severity of a vulnerability, SSVC focuses on the potential impacts of an exploitation for a specific organisation. It considers several factors such as exploitation status, technical impact, potential automation, mission prevalence, and public welfare impact. This framework is designed to help decision-makers determine how to manage an identified vulnerability. One of the key advantages of SSVC is its ability to prioritise risks specific to organisations, considering numerous factors unique to the organisation, such as system accessibility or the criticality of the affected assets. It proposes specific actions: monitor ("Track"), monitor closely ("Track*"), wait ("Attend"), or act immediately ("Act").

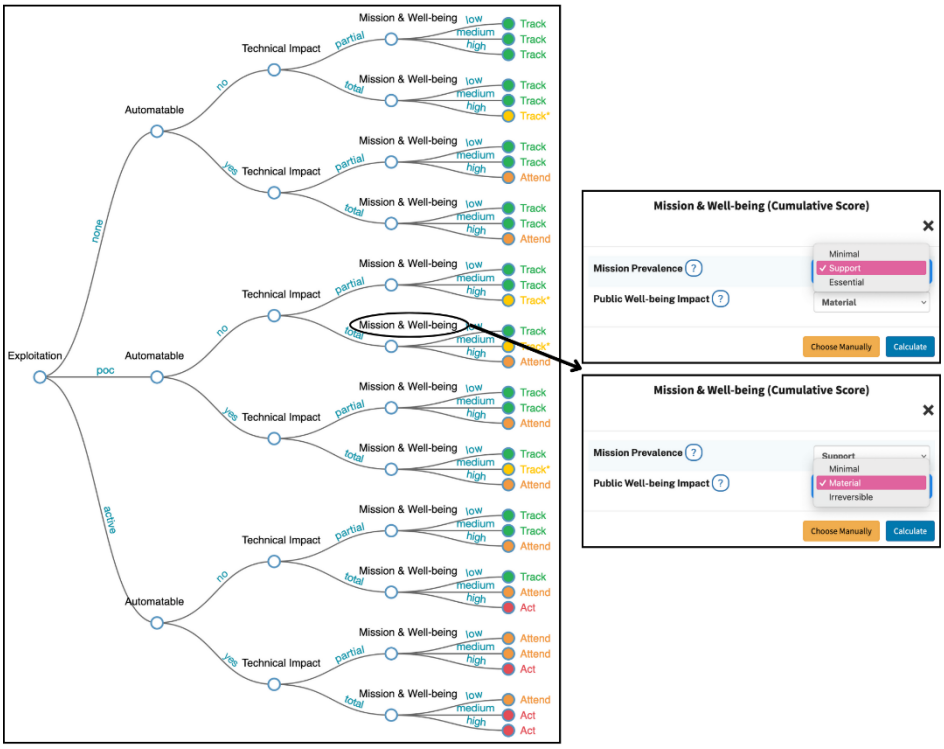

Figure 6: SSVC decision tree

To automate the implementation of the SSVC system within a vulnerability management process, it is crucial for the organisation to have sufficient maturity in managing asset inventory and their criticality. This requires precise and up-to-date knowledge of all assets present in the environment, as well as a thorough assessment of their importance to the company's strategic missions. Without clear visibility into critical assets and their potential impact if a vulnerability, automating SSVC could be ineffective or lead to incorrect prioritisation. Additionally, continuous monitoring and evaluation processes are necessary to adjust priorities according to environmental changes or newly discovered vulnerabilities. SSVC thus offers a more nuanced and personalised approach to vulnerability management, considering the specificities and priorities of each organisation.

4. Reliance or Independence

4.1 Divergences in Analysis Methods

Launched in 1999 by the MITRE Corporation, the CVE program is an initiative aimed at identifying, defining, and cataloguing publicly disclosed cybersecurity vulnerabilities. Its goal is to provide a common reference for vulnerabilities, thereby easing coordination among different cybersecurity stakeholders. As the primary publisher of the CVE program, MITRE Corporation oversees the entire process of assigning CVE identifiers. To efficiently manage the growing volume of vulnerabilities, it implemented a decentralised system in 2005, appointing CVE Numbering Authorities (CNAs) to assign CVE identifiers within their respective domains. These CNAs can be companies, organisations, or government agencies specialising in cybersecurity. They are responsible for publishing information related to these vulnerabilities, contributing to transparency and collaboration within the cybersecurity community. This collaboration led to a significant increase in the number of CVEs starting in 2005. Prior to this, just over 1,000 CVEs were published each year. In 2005, this number almost reached 7,000, and it has continued to grow, peaking at nearly 30,000 CVEs in 2023 as shown in Figure 1.

In parallel with the CVE program, a major player supports this initiative: the National Vulnerability Database (NVD). Maintained by the U.S. National Institute of Standards and Technology (NIST), the NVD is a comprehensive database that centralises and enriches information on vulnerabilities. Although the NVD is not the entity managing the CVE program, it plays a complementary role by providing detailed information on each identified vulnerability. For each CVE, the NVD adds metadata such as detailed descriptions, severity scores based on CVSS, references to solutions or patches, and information on affected products (CPE). While MITRE Corporation provides a standardised nomenclature to identify vulnerabilities, the NVD offers detailed information and analysis tools that ease the prioritisation of corrective actions. This constructive collaboration

allows organisations to strengthen their security posture by responding in a targeted manner to identified threats.

However, security teams often find themselves dealing with two distinct analyses: that of the vendor and that of the NVD. While these analyses may sometimes converge, divergences can occur, particularly regarding the CVSS scores assigned to CVEs. In the face of these differences, the question arises: "Whom should we refer to?" For consistency and reputation, the NVD's analysis is often favoured. However, this reliance on the NVD has started to cause problems since 2024.

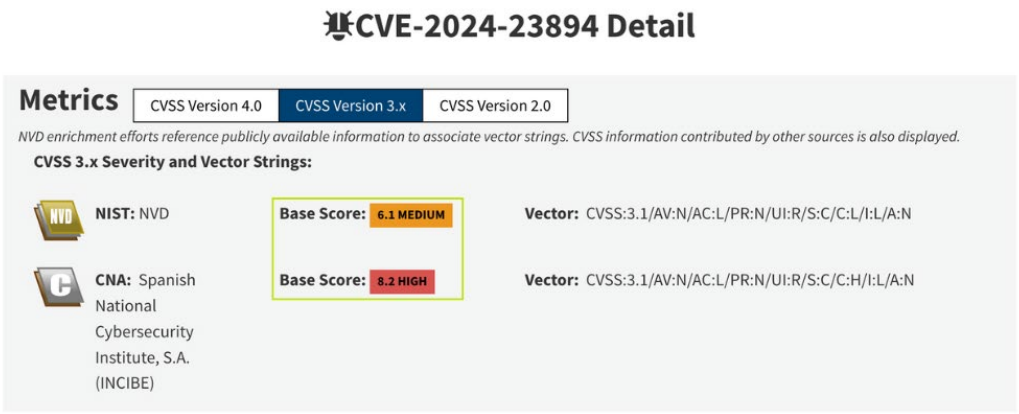

Figure 6: Differentiation of the CVSS score from CVE-2024-23894

It is important to remember that the CVSS score is designed to measure the impact of a vulnerability on a system. Although it is not the only factor to be considered when prioritising vulnerabilities, it remains a benchmark for many organisations today. A change in CVSS scores can significantly influence the prioritisation of vulnerabilities. In the absence of a structured prioritisation plan, organisations often tend to focus on vulnerabilities with a score above 8 in their patch management process. This disparity complicates the prioritisation process and can lead to critical vulnerabilities being overlooked and not addressed in time.

4.2 Reliance on the NVD

The NVD is still widely perceived as a reliable and neutral source, and its analyses are commonly used to prioritise patches. Its database is integrated into many vulnerability management tools and is a key resource for security teams. Today, however, the NVD is showing signs of saturation and is struggling to keep pace with the growing number of vulnerabilities, making it increasingly overwhelmed. Since the start of 2024, the NVD has announced delays in processing and enhancing new vulnerabilities. Many CVEs are therefore awaiting analysis, and those who had automated their vulnerability management via NVD are now faced with gaps in CVE tracking, making the task manual. For example, the Palo Alto CVE CVE-2024-9468 rated with a CVSS-B (v4.0) at 8.2 by the vendor, published in September 2024, has still not been analysed four months later, either in CVSS v3.x or v4.0 by the NVD.

On February 13, 2024, the NVD announced that it was working on a consortium to improve the NVD Program, with a primary focus on analysing only the most critical vulnerabilities for the time being. During the VulnCon 2024 conference in March, Tanya Brewer, head of the NVD, described the situation as a "government issue". Tom Alrich, a cybersecurity consultant and leader of the OWASP SBOM forum, clarified on his blog that the problem stems mainly from organisational challenges between U.S. agencies, such as the Department of Commerce and the Department of Homeland Security, making its resolution politically complex. To address this issue, the CISA launched the "Vulnrichment" program in May 2024. The goal of this program is to enrich CVE records with contextual data to improve vulnerability management. Available on GitHub, each enriched CVE is provided in JSON format, easing its integration into organisations' vulnerability management processes. By that time, CISA had already enriched 1,300 CVEs with more detailed information provided by the CNAs. Additionally, thanks to their SSVC analysis method, they are now better equipped to assess the exploitation status, security impact, and prevalence of affected products. In July 2024, the NVD announced it would incorporate CISA's enriched data into its own records, allowing for better information consolidation and improved coordination among entities involved in vulnerability management.

By the end of 2024, the NVD reported over 20,000 unenriched CVEs. Given that between 25,000 and 30,000 CVEs have been published annually since 2022, this means almost two-thirds of the 2024 CVEs remained

unanalysed. According to available data, about 72.4% of the CVEs published between February 12 and September 21, 2024, have not yet been analysed by the NVD. This slowdown in the NVD's CVE analysis highlights a significant issue: the excessive reliance on a single entity for processing and enriching vulnerabilities. Although the NVD is a key player in global vulnerability management, its current delays expose the fragility of a centralised model that relies on one institution to ensure the prompt update of critical cybersecurity information. This bottleneck directly affects businesses and organisations that depend on these data to automate their vulnerability management and deploy corrective measures in real-time.

The current situation also raises concerns about system resilience. In case of failure or delays within the NVD, organisations are unable to effectively manage the risks associated with newly discovered vulnerabilities. This lack of responsiveness can lead to prolonged exposure to threats, jeopardising the security of critical systems. While solutions like CISA's "Vulnrichment" program have been implemented to fill these gaps, they are not enough to fully compensate for the void left by the NVD, and the reliance on a single actor stays a significant challenge.

4.3 Towards Independence in Evaluation

The slowdown observed by the NVD and the growing dependence on a single entity to process CVEs underline the importance of independence in vulnerability assessment. However, independence is not an easy task, and there are several challenges to overcome on the road to autonomous, decentralised vulnerability management.

To begin with, it is essential to broaden the sources of information. Today, variety of players, both public and private, specialise in publishing CVEs. However, there are significant disparities in the quantity and quality of information from one CVE to another. For example, if we consider the total number of CVEs published in 2023, no one agrees on a single figure. Consequently, the more diversified the identification channels, the lower the risk of missing important vulnerabilities.

Table 1: Number of CVEs in 2023

MITRE	NVD (cve.icu)	CVEDetails	OpenCVE	Vulnrichment
28961 published CVE records + 40051 reserved CVE IDs	28818	29066	29093	14872

For MITRE, reserved CVE IDs refer to CVEs that have been identified and assigned an identifier but whose details have not yet been published. Published CVE records are those whose details have been made public and are accessible.

The second point, as mentioned above, concerns the diversity of indicators to be used to effectively prioritise the remediation of vulnerabilities in a given environment. The CVSS score alone is no longer sufficient and is showing its limitations. Is it really that decisive? For example, if you work in a totally isolated environment and a CVE with a critical CVSS score signals an XSS vulnerability in the web portal of one of your applications, is it necessary to immediately interrupt all activities to correct it, when the attacker could only exploit it by accessing the local network? It's time to move beyond this CVSS score-centric vision and focus on a truly contextual analysis. The use of other indicators, such as EPSS or SSVC, makes it possible to refine prioritisation: by identifying which software and hardware assets are really at risk and directing monitoring accordingly, rather than basing it on a fixed CVSS threshold, management can become more proactive. By structuring a hierarchy of prioritised assets and using streams of CVE information from multiple sources, analysts can focus on vulnerabilities affecting critical assets and re-prioritise each CVE considering a more relevant contextual analysis than that provided by the CVSS score alone.

A good example of this is the curl project, which abandoned the use of CVSS to assess the seriousness of its vulnerabilities, because it did not allow specific contexts of use to be taken into account, as was the case with the CVE CVE-2024-11053, which curl's experts judged to be minor and which was wrongly classified as critical by CISA, illustrating the limits of the blind use of standardised scores.

Although this approach requires significant effort to implement effective automation, in the long term it will offer a more complete vision that is less dependent on a single source or tool. The real question remains: what is most relevant for each organisation? Should they invest in open resource automation based on their scope, or opt for a commercial tool already available on the market? This decision needs to be tailored to the priorities of each organisation, because the aim is not to provide a universal answer, but to determine what is best for the organisation's security. In addition, security teams must not overlook the importance of monitoring, particularly

through Cyber Emergency Response Teams (CERTs) or publishers' publications. This monitoring enables them to stay informed in real time and avoid becoming over-dependent on tools or automated systems that may also present vulnerabilities.

5. Conclusion

In an increasingly connected world, vulnerability management has never been more critical. While frameworks such as CVSS have provided a solid basis for assessing the severity of vulnerabilities, they are no longer sufficient on their own. Tools such as EPSS and SSVC are emerging as promising additions to organisations' prioritisation strategies. However, as the delays in the 2024 NVD show, they need to develop their own assessment capabilities and make use of a variety of data sources. By diversifying their approaches and strengthening their internal analysis processes, they will not only be able to reduce their dependence on third parties but also maximise their resilience in the face of constantly evolving cyber threats.

References

Alrich, T. (2024). It's time to move beyond the NVD. [online] Blogspot.com. Available at: https://tomalrichblog.blogspot.com/2024/03/its-time-to-move-beyond-nvd.html [Accessed 4 Jan. 2025].

Carneige Mellon University (2025). Software Engineering Institute. [online] www.sei.cmu.edu. Available at: https://sei.cmu.edu/ [Accessed 3 Jan. 2025].

CISA (2020). Cybersecurity & Infrastructure Security Agency. [online] Cisa.gov. Available at: https://www.cisa.gov/ [Accessed 14 Dec. 2024].

CISA (2024). Stakeholder-Specific Vulnerability Categorization (SSVC). [online] www.cisa.gov. Available at: https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc [Accessed 14 Dec. 2024].

cisagov (2024). CISA Vulnrichment. [online] GitHub. Available at: https://github.com/cisagov/vulnrichment [Accessed 4 Jan. 2025].

curl (2024). curl - netrc and redirect credential leak - CVE-2024-11053. [online] Curl.se. Available at: https://curl.se/docs/CVE-2024-11053.html [Accessed 25 Jan. 2025].

CVE (2025). cve-website. [online] www.cve.org. Available at: https://www.cve.org/ [Accessed 14 Dec. 2024].

CVE Details (2024). CVE Details. [online] Cvedetails.com. Available at: https://www.cvedetails.com/ [Accessed 14 Dec. 2024].

FIRST (2015). FIRST - Improving Security Together. [online] FIRST — Forum of Incident Response and Security Teams. Available at: https://www.first.org/ [Accessed 14 Dec. 2024].

FIRST (2019). Common Vulnerability Scoring System SIG. [online] FIRST — Forum of Incident Response and Security Teams. Available at: https://www.first.org/cvss/ [Accessed 14 Dec. 2024].

FIRST (2021a). EPSS User Guide. [online] FIRST — Forum of Incident Response and Security Teams. Available at: https://www.first.org/epss/user-guide [Accessed 14 Dec. 2024].

FIRST (2021b). The EPSS Model. [online] FIRST — Forum of Incident Response and Security Teams. Available at: https://www.first.org/epss/model [Accessed 14 Dec. 2024].

Gamblin, J. (2025). CVE.ICU. [online] Cve.icu. Available at: https://cve.icu/intro.html [Accessed 14 Dec. 2024].

Haxx, D. (2025). CVSS is dead to us. [online] daniel.haxx.se. Available at: https://daniel.haxx.se/blog/2025/01/23/cvss-is-dead-to-us/ [Accessed 25 Jan. 2025].

MITRE (2013). CPE - Common Platform Enumeration: About CPE. [online] Mitre.org. Available at: https://cpe.mitre.org/about/ [Accessed 14 Dec. 2024].

MITRE (2019). CVE - Common Vulnerabilities and Exposures (CVE). [online] Mitre.org. Available at: https://cve.mitre.org/ [Accessed 14 Dec. 2024].

MITRE (2024a). About the CVE Program. [online] www.cve.org. Available at: https://www.cve.org/About/Overview [Accessed 14 Dec. 2024].

MITRE (2024b). CVE Numbering Authorities (CNAs). [online] www.cve.org. Available at: https://www.cve.org/ProgramOrganization/CNAs [Accessed 14 Dec. 2024].

MITRE (2024c). CWE - Common Weakness Enumeration. [online] cwe.mitre.org. Available at: https://cwe.mitre.org/ [Accessed 14 Dec. 2024].

NIST (2019). National Vunerability Database. [online] Nist.gov. Available at: https://nvd.nist.gov/ [Accessed 14 Dec. 2024].

NIST (2024). National Institute of Standards and Technology. [online] NIST. Available at: https://www.nist.gov/ [Accessed 14 Dec. 2024].

NVD (2024a). NVD - CVE-2024-9468. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln/detail/cve-2024-9468 [Accessed 14 Dec. 2024].

NVD (2024b). NVD - CVE-2024-23894. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2024-23894 [Accessed 14 Dec. 2024].

NVD (2024c). NVD - CVE-2024-29824. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln/detail/cve-2024-29824 [Accessed 14 Dec. 2024].

NVD (2024d). NVD Dashboard. [online] nvd.nist.gov. Available at: https://nvd.nist.gov/general/nvd-dashboard [Accessed 14 Dec. 2024].

NVD (2024e). NVD Updates. NIST. [online] Available at: https://www.nist.gov/itl/nvd [Accessed 14 Dec. 2024].
OpenCVE (2024). OpenCVE - Opensource Vulnerability Management Platform. [online] Opencve.io. Available at: https://www.opencve.io/ [Accessed 14 Dec. 2024].
OWASP (2020). Cross Site Scripting (XSS). [online] Owasp.org. Available at: https://owasp.org/www-community/attacks/xss/ [Accessed 20 Mar. 2025].
Palo Alto Networks Security (2024). CVE-2024-9468 PAN-OS: Firewall Denial of Service (DoS) via a Maliciously Crafted Packet. [online] Paloaltonetworks.com. Available at: https://security.paloaltonetworks.com/CVE-2024-9468 [Accessed 14 Dec. 2024].
Sager, T. (2015). The Cyber OODA Loop: How Your Attacker Should Help You Design Your Defense.