Adoption of CVSS v4.0 vulnerability assessment calculator

BY ELEANOR BARLOW · MAY 28, 2025 · LAST UPDATED ON FEBRUARY 20, 2026

What you will learn

- **What the Common Vulnerability Scoring System (CVSS) v4.0 is and how it improves vulnerability severity assessment** compared with previous versions, including its expanded metrics and more granular scoring methodology.
- **Why adopting CVSS v4.0 matters for more accurate risk prioritization and security decision making**, and how organizations can leverage its enhanced definitions for impact, threat, and environmental factors.
- **How Intigriti has implemented CVSS v4.0 within its platform** and what this means for vulnerability triage, severity alignment, and remediation going forward.

CVSS stands for "Common Vulnerability Scoring System". The CVSS framework is an open cyber security framework owned by a US-based non-profit organization "Forum of Incident Response and Security Teams" (FIRST). The mission of FIRST is to help worldwide cyber security response teams quickly and easily calculate the severity of cyber security vulnerabilities based on metrics.

How it works

There have been multiple versions and adaptations of the framework. The latest version (4.0) is designed to assess the severity of security vulnerabilities across multiple environments and dimensions, including exploitability, impacts, and more, and provide a numerical score of said vulnerabilities.

The score is based on three key groups:

1. **Base** – This represents intrinsic elements that are constant over time and across environments.
2. **Threat** – This represents characteristics of vulnerabilities that change over time.
3. **Environmental** – This represents characteristics of vulnerabilities that are unique to an environment.

When all these elements are combined, metrics are generated and aligned with real-world attack patterns and risk management to reflect the vulnerability severity level which, in turn, means that response actions can be prioritized. This helps organizations with the age-old problem of prioritization and gives them the data to rank and grade patches and vulnerabilities as they are discovered. These changes improve the overall usability of CVSS, in comparison to previous versions.

"Regarding prioritization, the usefulness of a numerical CVSS score is directly proportional to the CVSS metrics leveraged to generate that score. Therefore, numerical CVSS scores should be enumerated using nomenclature that communicates the metrics used in its generation."- First.org

There is an additional group now available in version 4.0, termed **"Supplemental",** and this represents characteristics that supplement metrics. This supplementary material does not, however, impact the final score, but provides additional context.

The value of CVSS v4.0 compared to v3.0

CVSS v4.0 brings improved granularity in scoring, better alignment with real-world risk assessments, and additional metrics that help organizations make more informed security decisions. With clearer severity assessments, both researchers and organizations benefit from a more consistent and transparent evaluation process. Version 4.0 provides an enhanced view and representation of real-world risk by introducing new elements such as mitigation efforts and recovery, that transform the ability to learn, adapt, and grow, as well as customize to the needs and challenges of the user.

There are many differentiators between CVSS v3.0 and CVSS v4.0. According to the information provided on the FIRST.ORG website, changes include the following:

- **Scope Removed.** The concept of Scope has been replaced with the concepts of a vulnerable system (VC, VI, VA) and a subsequent system (SC, SI, SA), capturing impacts from both, where relevant.
- **Assessing Vulnerabilities in Software Libraries (and Similar).** New guidance explains how to assess the impact of a vulnerability in a library.
- **Multiple CVSS Base (CVSS-B) Scores**. Guidance explicitly allows multiple CVSS Base Scores to be generated for a vulnerability that affects multiple product versions, platforms, and/or operating systems.
- **Guidance for Using Environmental Security Requirements Metrics**. The Environmental Metric Group includes three Security Requirement metrics: Confidentiality Requirement of the vulnerable system (CR), Integrity Requirement of the vulnerable system (IR), and Availability Requirement of the vulnerable system (AR).

CVSS v4.0 and other scoring systems

There are multiple types of scoring systems in the cyber security space. Many frameworks are essential to meet compliance and regulations and can be combined to provide a rounded view of security posture.

- **NIST** – The National Institute of Standards and Technology framework was developed to help businesses identify, manage, and reduce risks using functions to identify, protect, detect, respond, and recover. While the framework was initially intended to support and protect US-based infrastructure for the United States Department of Defense, it is now used as a framework, across multiple industries around the world.
- **MIRE ATT&CK Framework** – The MITRE ATT&CK framework serves as a knowledge base of adversary tactics, techniques, and procedures (TTPs) and has a "mission to solve problems for a safer world, by bringing communities together to develop more effective security". These TTPs are based on real-world observations, made globally accessible, and used as the foundation for threat models and methodologies. This model is heavily used in the private sector and for governmental entities.
- **OWASP**- The Open Web Application Security Project is a foundation that aims to improve the security of software by providing a ‘Top 10’ list of the most critical web application risks. Security researchers

and bug bounty hunters alike often regard the OWASP top 10 as the official ranking for defining the top 10 most critical web application security risks.

- **EPSS**- The Exploit Prediction Scoring System was created by FIRST to estimate the likelihood that a vulnerability will be targeted in the wild. The goal is to prioritize vulnerabilities, provide severity measures, and bridge the gap between threat information and real-world exploit data. The model is formulated so that a score is provided for the probability of each vulnerability. The higher the number, the higher the likelihood that the vulnerability will be exploited.

- **DREAD**- 'Damage, Reproducibility, Exploitability, Affected Users, and Discoverability' is a framework created by Microsoft to assess the severity of threats that have already been identified. The score-based system is used to measure the potential severity of the identified threat. It often works in tandem with the 'Process for Attack Simulation' (PASTA) and "Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege" (STRIDE) frameworks.

Each of these frameworks has its own merits. But what makes CVSS 4.0 beneficial for vulnerability scoring is that new base metrics and values have been added to provide visibility and granularity of impact metrics.

Intigriti's introduction of CVSS 4.0

While the CVSS v3.0 calculator has been a reliable standard, CVSS v4.0 provides a precise and comprehensive vulnerability assessment that gives customers greater flexibility in how they assess and prioritize vulnerabilities, ensuring alignment with evolving security needs and risk management strategies.

> **"With the introduction of CVSS 4.0, our goal is to offer customers improved accuracy in assessing vulnerabilities, helping them prioritize remediation efforts more effectively. The enhanced scoring system of CVSS 4.0 allows for more precise vulnerability assessments, fostering better alignment of rewards for researchers and enabling organizations to make more informed decisions regarding remediation and resource allocation."**
>
> **Inti De Ceukelaire, Chief Hacker Officer, Intigriti**

Yannick Merckx, Product Marketing Manager, at Intigriti, also noted that

> **"We will continue to monitor industry trends and evolving customer needs to ensure our platform not only remains compliant with best practices and emerging standards but also anticipates future demands. With CVSS 4.0 now thoroughly tested and already adopted by a significant portion of our customer base, we're fully committed to supporting them throughout this transition, providing the necessary tools and platform enhancements."**

Considerations and next steps

The calculator is available to all Intigriti customers. Configuration is set at the company level, meaning all programs within the organization adopt the new severity assessment method. Companies can switch to CVSS 4.0 whenever they are ready.

For more information regarding our adoption of CVSS 4.0, read this blog, or contact the team here.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.