CVSS 4.0 is Here: How to Make the Most of It

AJ Starita • February 7, 2024 • 5 min read

Application Security

Share article

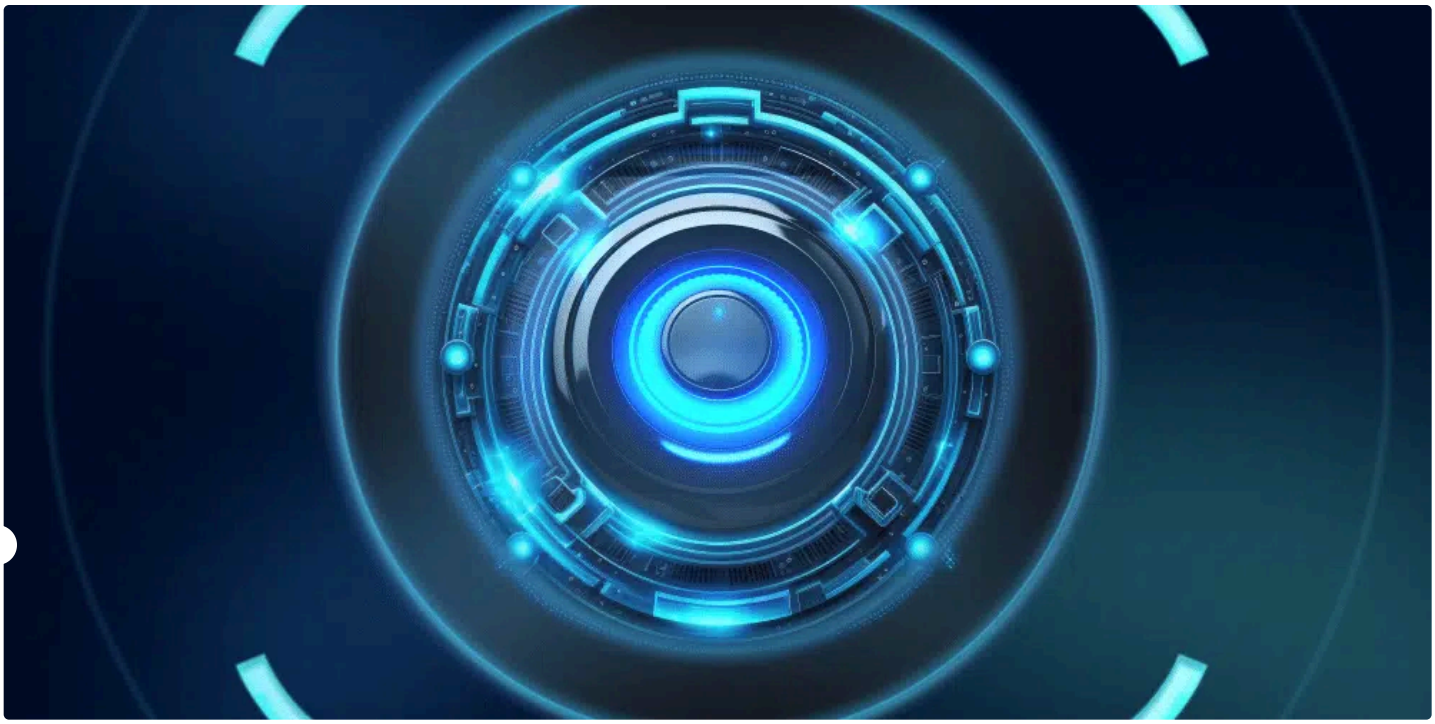

Table of Contents

The CVSS (Common Vulnerability Scoring System) is a widely used standard that produces a score between 0 and 10 to indicate the level of severity of a vulnerability. The most popular spot to find CVSS scores is on the National Vulnerability Database (NVD) website, where you'll see CVSS scores for all CVE (Common Vulnerabilities and Exposures) IDs. For any given CVE on the NVD website, the base CVSS score, which is created from data provided by suppliers, can be altered with additional context in order to reveal a new overall score that's specific to your organization's situation.

The Forum of Incident Response and Security Teams (FIRST) manages the CVSS, which is updated and promoted by a special interest group (SIG) composed of individuals and organizations from a broad range of industries and academia. The first version of CVSS was released in 2005 and after a period of public comment, the latest version was released in November of 2023.

CVSS scores are frequently employed as a large or small part of an organization's policy for prioritizing vulnerabilities to remediate, so having CVSS scores that reflect real-world risk is important.

What's new?

While CVSS 4.0 is significantly different from its predecessors, we will limit our focus to some of the biggest changes. The most visually obvious change is that CVSS 4.0 takes in many more details than CVSS 3.1. These new or reshaped measurements give finer granularity to the base metrics and include Attack Complexity, Attack Requirements, and enhancements to User Interaction.

Here is a quick breakdown of the new metrics in Common Vulnerability Scoring System Version 4.0.

Attack Complexity	Reflects the exploit engineering complexity required to evade or circumvent defensive or security-enhancing technologies
Attack Requirements	Reflects the prerequisite conditions of the vulnerable component that makes an attack possible
Automatable	Whether or not an attacker can automate the exploit across multiple targets
Recovery	The resilience of a component or system to recover performance and availability of services after an attack
Value Density	The resources over which an attacker will gain control with a single exploitation event, either diffuse (small) or concentrated (rich in resources)
Vulnerability Response Effort	How difficult it is for consumers to respond to the impact of vulnerabilities for deployed products and services in their infrastructure on a scale of low, medium, and high
Provider Urgency	Enables any provider along the software supply chain to supply an additional assessment of risk and urgency on a green/amber/red scale of rising severity
Safety	The impact regarding the safety of a human actor or participant that can be predictably injured as a result of the vulnerability being exploited

At first blush, the inclusion of so many new parameters makes CVSS 4.0 seem more complex and harder to work with, but these new variables serve to simplify and refine the system, as well as to provide clearer definitions and guidance in order to reduce subjectivity and confusion.

With these new measurements, CVSS 4.0 scores weigh exploitability and context more heavily in order to better reflect true severity. This means most scores go down in CVSS 4.0 compared to CVSS 3.1, which is excellent news for organizations with policies to remediate all CVEs with scores above a certain number. Exploited vulnerabilities maintain their high scores or even go up.

Some changes to the CVSS come in the form of removing metrics. The Scope metric, which sought to measure the ability of a vulnerability in a software component to impact other software or hardware outside of the same security

authority or scope, has been retired. This phenomenon is now reflected in Impact Metrics, which includes confidentiality, integrity, and availability metrics for both vulnerable systems and subsequent systems. Additionally, Remediation Level, Report Confidence, and Exploit Code Maturity were simplified to Exploit Maturity.

Mend SCA is the first to feature CVSS 4.0 scores. Where else can they be found?

At the time of this writing, CVSS 4.0 scores aren't available in many places. You can calculate them yourself here, but the NVD is not expected to adopt CVSS 4.0 for new CVEs until sometime in the first half of this year, though no official word has come down yet. Because the NVD didn't add CVSS 3.0 scores to old CVEs when the jump was made from 2.0, we don't expect recalculations of older CVEs once the NVD begins using 4.0 either.

If you're a user of our software composition analysis (SCA) tool, you're in luck. Mend SCA is the first to include CVSS 4.0 scores. We've already done the recalculations necessary to include CVSS 4.0 scores for all CVEs and we will continue to provide CVSS 3.1 and 2.0 scores as well so you're covered no matter what your organization's policies are.

How should I use CVSS 4.0 scores?

As with earlier versions, CVSS 4.0 is designed to help you recognize the impact of CVEs encountered in your software development pipeline. Version 4.0's enhanced clarity, flexibility, granularity, and usability make it a valuable tool for identifying vulnerabilities and assessing their risks and threats, so we encourage you and your developers to consider it across the software development lifecycle.

If you have a mature AppSec program that is already using CVSS 3.1 scores wisely, you should use CVSS 4.0 scores in much the same way. But it's important to remember that the CVSS scores you'll usually see reported in the NVD and in automated reports from your security software are base scores.

While the base scores of CVSS 4.0 are better reflections of severity than those of its predecessors, a base score only tells you so much. Many of the metrics that are new in CVSS 4.0 are not to help software suppliers report vulnerabilities but to help you, the consumer, adjust the final score to reflect your particular situation. FIRST recommends you use asset management databases for environmental metric values and threat intelligence data for threat metric values.

Along with tools with reachability path analysis like Mend SCA, other scoring systems like EPSS, and good application security practices such as keeping robust software inventories, CVSS 4.0 is an extremely beneficial component of an effective risk assessment and prioritization program.

About the author

AJ Starita