UNDERSTANDING CVSS SCORES

CVSS scores are commonly used by infosec teams as part of a vulnerability management program to provide a point of comparison between vulnerabilities, and to prioritize remediation of vulnerabilities.

But exactly what are they and how are they calculated?

WHAT IS CVSS?

The Common Vulnerability Scoring System (CVSS) is an open framework maintained by the Forum of Incident Response and Security Teams (FIRST), a US-based nonprofit with over 500 member organizations globally.

It provides a numerical (0-10) representation of the severity of an information security vulnerability.

CVSS V3

CVSS is now on its third major version (v3.1), which was designed to address some of the shortcomings in its predecessor, v2. Most notably, version 3 introduces the looks at the privileges required to exploit a vulnerability, as well as the ability for an attacker to propagate across systems ("scope") after exploiting a vulnerability.

CVSS SCORE METRICS

A CVSS score is composed of three sets of metrics (**Base**, **Temporal**, **Environmental**), each of which have an underlying scoring component.

BASIC METRIC GROUP

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope

Impact Metrics

- Compatibility Impact
- Integrity Impact
- Availability Impact
- Scope

TEMPORAL METRIC GROUP

- Exploit Code Maturity
- Remediation Level
- Report Confidence

ENVIRONMENTAL METRIC GROUP

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement
- Modified Base Metrics

CVSS BASE METRICS

Base Factors represent characteristics of the vulnerability itself. These characteristics do not change over time and are not dependent on real world exploitability or on compensating factors that an enterprise has put into place to prohibit exploit.

> Public rankings of severity, such as those listed in NIST's National Vulnerability Database (NVD) refer exclusively to Base CVSS scores.

The easy availability of Base CVSS scores provides a seductive starting point for patching prioritization but is of limited use as it does not account for real world exploits, availability of patches, or other environmental or mitigating controls that your organization has put into place.

EXPLOITABILITY

Exploitability metrics are made up of characteristics of the vulnerable component, with Exploitability being made up of four further sub-components.

- **Attack Vector—**Based on the level of access required to exploit a vulnerability.
- **Attack Complexity—**Based on the factors outside of the attacker's control that are required to exploit the vulnerability.
- **Privileges Required—**this score varies based on the privileges required for the attacker to conduct the exploit.
- **User Interaction—**this score varies based on whether the attacker must recruit either a willing or unwitting participant in order to complete their task.

SCOPE

Scope relates to whether a vulnerability in one component can propagate to other components.

IMPACT

Impact focuses on the actual outcome that an attacked can achieve as a result of exploiting the vulnerability in question. Impact metrics are comprised of three sub-metrics.

- **Confidentiality—**Based on the amount of data that the attacker gains access to.
- **Integrity—**Based on the ability of the attacker to alter or change data on the impacted system.
- **Availability—**Based on the loss of availability of the exploited system.

CVSS TEMPORAL METRICS

These metrics are related to a vulnerability that change over time. They measure the current exploitability of the vulnerability, as well as the availability of remediating controls, such as a patch.

- **Exploit Code Maturity—**Until a method exists to exploit a vulnerability, it is relatively benign. As with most software, code available to conduct an exploit can mature, becoming more stable and more widely available over time. As this happens, the score on this subcomponent will increase.
- **Remediation Level—**When a vulnerability is first discovered, there might not be a patch or other workaround available. Over time, workarounds, temporary fixes, and ultimately official patches become available, lowering the vulnerability score as remediation is improved.
- **Report Confidence—**Confidence measures the level of validation demonstrating that a vulnerability is both real and exploitable.

CVSS ENVIRONMENTAL METRICS

Environmental Metrics allow the organization to modify the Base CVSS based on Security Requirements and modifications of Base Metrics

- **Security Requirements—**These characterize the criticality of the asset in question.
- **Modified Base Metrics—**An organization may choose to modify values of the Base CVSS Metrics based on mitigations that they have put into place.

CVSS QUALITATIVE RATINGS

CVSS Score	Qualitative Rating
0.0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

WHAT IS THE DIFFERENCE BETWEEN CVSS AND CVE?

CVE stands for Common Vulnerability Enumeration, which is a unique identifier for each vulnerability listed in the NIST NVD.

CVSS provides an indication of the severity of each CVE.

LIMITATIONS OF CVSS

Publicly available CVSS scores are Base Scores only. They represent the severity of a vulnerability, but do not reflect the risk that the vulnerability poses to your environment. In other words, CVSS answers the question, "Is this dangerous?", but not, "Is this dangerous to my company?"

Given the large (and growing) number of vulnerabilities facing the typical organization, effective vulnerability management must account for not only the Base Score, but Temporal and Environmental Factors as well.

GOING BEYOND CVSS

NIST can't help you with tailoring your CVSS score to above factors, as they require first-hand knowledge of business criticality of the assets, identification of mitigating controls, use of the asset in question, and current real-world exploitability of the vulnerability. Maximizing efficiency of your security team requires a risk-based approach to vulnerability management that accounts for these factors.