Common Vulnerability Scoring System (CVSS) v4.0 Specification Summary

by Atsu Vovor[i]

Overview

In this article, we will try to summarize as much as possible the CVSS V4.0 published on the FiRST[ii] website. The Common Vulnerability Scoring System (CVSS) is a standardized framework for assessing the severity of security vulnerabilities in information systems. Version 4.0 (CVSS v4.0), released in November 2023, introduces several enhancements to improve the accuracy and applicability of vulnerability assessments

Key Features of CVSS v4.0

Metric Groups

CVSS v4.0 evaluates vulnerabilities across four primary metric groups:

Base Metrics: Assess the intrinsic characteristics of a vulnerability that are constant over time and across user environments.

Temporal Metrics: Consider factors that may change over time but are independent of user environments, such as the availability of exploit code or the existence of a fix.

Environmental Metrics: Account for the unique characteristics of a user's environment, including security requirements and potential impacts.

Supplemental Metrics: Provide additional context to refine the overall severity score, offering a more nuanced understanding of the vulnerability.

Attack Requirements Metric

This new metric complements the existing Attack Complexity metric by evaluating conditions on the target side necessary for exploitation, enhancing the precision of vulnerability assessments.

Impact Metrics Refinement

CVSS v4.0 distinguishes between impacts on the vulnerable system itself and impacts on subsequent systems, replacing the previous Scope metric to offer a clearer understanding of potential consequences.

Extended Base Metrics

The Base Metrics group now includes:

Attack Vector (AV): Describes the context by which vulnerability exploitation is possible.

Attack Complexity (AC): Assesses the conditions beyond the attacker's control that must exist for exploitation.

Attack Requirements (AT): Evaluates necessary conditions on the target side for exploitation.

Privileges Required (PR): Determines the level of privileges an attacker must possess before successfully exploiting the vulnerability.

User Interaction (UI): Indicates whether exploitation requires interaction from a user other than the attacker.

Vulnerable System Impact Metrics:

Confidentiality Impact (VC): Measures the impact on confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability.

Integrity Impact (VI): Measures the impact on integrity.

Availability Impact (VA): Measures the impact on availability.

- **Subsequent System Impact Metrics:**
    - **Confidentiality Impact (SC):** Assesses the impact on confidentiality of subsequent systems.
    - **Integrity Impact (SI):** Assesses the impact on integrity of subsequent systems.
    - **Availability Impact (SA):** Assesses the impact on availability of subsequent systems.

Key Features of CVSS v4.0 Summary Table

Feature	Description
Metric Groups	• **Base Metrics:** Intrinsic characteristics constant over time. • **Temporal Metrics:** Factors changing over time (e.g., exploit availability). • **Environmental Metrics:** User-specific characteristics and impacts. • **Supplemental Metrics:** Additional context for refining severity.
Attack Requirements Metric	Evaluates target-side conditions necessary for exploitation.
Impact Metrics Refinement	Distinguishes between impacts on vulnerable systems and subsequent systems.
Extended Base Metrics	• **Attack Vector (AV):** Context enabling exploitation. • **Attack Complexity (AC):** Conditions beyond attacker's control. • **Attack Requirements (AT):** Target-side necessary conditions. • **Privileges Required (PR):** Level of attacker privileges required. • **User Interaction (UI):** User involvement required for exploitation.
Vulnerable System Impact Metrics	• **Confidentiality Impact (VC):** Impact on system confidentiality. • **Integrity Impact (VI):** Impact on system integrity. • **Availability Impact (VA):** Impact on system availability.
Subsequent System Impact Metrics	• **Confidentiality Impact (SC):** Impact on subsequent system confidentiality. • **Integrity Impact (SI):** Impact on subsequent system integrity. • **Availability Impact (SA):** Impact on subsequent system availability.

The enhancements in CVSS v4.0 aim to provide a more comprehensive and precise assessment of vulnerabilities, facilitating better risk management and mitigation strategies.

---

[i] Atsu Vovor: Consultant, Data & Analytics Specialist | Machine Learning | Data science | Quantitative Analysis | French & English Bilingual | atsu.vovor@bell.net | https://github.com/atsuvovor/Pub_Data_Analytics_BilingProject | https://public.tableau.com/app/profile/atsu.vovor8645/vizzes

[ii] Source: https://www.first.org/cvss/v4.0/specification-document#:~:text=The%20Common%20Vulnerability%20Scoring%20System,Threat%2C%20Environmental%2C%20and%20Supplemental.