I. Introduction

The Common Vulnerability Scoring System (CVSS) version 4.0 is the latest iteration of the industry-standard scoring system for assessing and quantifying the severity and impact of software vulnerabilities.

CVSS v4.0 introduces several significant changes and improvements over the previous version (v3.1) to provide a more granular, accurate, and comprehensive assessment of vulnerabilities.

II. Key changes

Key Updates in CVSS v4.0 as for now:

- **New Base Metrics and Values**: CVSS v4.0 introduces new base metrics that capture additional aspects of risk, such as the potential consequences of a successful attack, including explicit assessment of impact to Vulnerable System (VC, VI, VA) and Subsequent Systems (SC, SI, SA)
- **Simplified Threat Metrics**: The Temporal Score has been renamed to Threat Metric Group and now includes only one metric, which is Exploit Maturity
- **New Supplemental Metric Group**: This group is introduced for Enhanced Extrinsic Attributes, providing additional insight into the characteristics of a vulnerability
- **Changes to Vector String**: The Vector String has been updated to begin with CVSS:4.0 rather than CVSS:3.1. Although no other changes have been made to the Vector String, CVSS v4.0 contains changes to the definition of some of the metric values and to the formulas
- **Improved Guidance**: CVSS v4.0 provides improved guidance to CVSS analysts to produce consistent scores. It also provides guidance on scoring vulnerabilities in software libraries and supports multiple CVSS scores for the same vulnerability that affects different platforms or operating systems
- **Enhanced Clarity and Simplicity**: CVSS v4.0 aims to provide a more streamlined scoring process, reducing subjectivity through clearer metric guidance and definitions
- **Focus on Resiliency**: The latest iteration of CVSS introduces a renewed focus on resiliency, particularly in the early stages of an exploit, addressing the increasing concerns around the security of operational technology (OT), industrial control systems (ICS), and the Internet of Things (IoT)
- **Renaming of Key Metrics**: The Temporal metrics in CVSS 3.1 have been renamed to Threat Metrics in CVSS 4.0
- **User Interaction**: CVSS 4.0 has made the User Interaction metric more granular. While CVSS 3.1 had the values None (N) or Required (R) for this metric, CVSS 4.0 has expanded the options to Active, Passive, and None
- **New Base Metrics and Values**: CVSS 4.0 introduces new base metrics and values, providing a more granular and accurate assessment of vulnerabilities
- **Assessing Effects on Vulnerable and Subsequent Systems**: CVSS 4.0 provides clearer insight into the impact of vulnerabilities on both the vulnerable system and subsequent systems
- **Simplifying Threat Metrics**: The Threat metrics in CVSS 4.0 have been simplified to focus only on Exploit Maturity
- **New Supplemental Metric Group**: CVSS 4.0 introduces a new Supplemental Metric Group for Enhanced Extrinsic Attributes
- **Attack Requirements**: CVSS 4.0 introduces a new base metric, "Attack Requirements", which gets the value "Present" if there is a pre-attack requirement
- **Scope Changes**: The "Scope" feature from CVSS v3.1 was retired and replaced with the concepts of "Vulnerable System" and "Subsequent System"
- **Support for Multiple Scores**: CVSS 4.0 is designed to support multiple CVSS scores for the same vulnerability that affects different platforms, operating systems, etc
- **Guidance for Other Sectors**: CVSS 4.0 provides guidance to extend the CVSS framework for other industry sectors such as privacy, automotive, etc

III. Benefits of using CVSS v4.0 over previous versions

CVSS v4.0 improves vulnerability assessments by introducing several enhancements that provide a more nuanced and accurate representation of the risks associated with software vulnerabilities:

- **More Granular Base Metrics** – CVSS v4.0 includes new base metrics and values that capture additional

aspects of risk, such as the potential consequences of a successful attack. This includes explicit assessment of impact to Vulnerable System (VC, VI, VA) and Subsequent Systems (SC, SI, SA), which allows for a more detailed understanding of the vulnerability's impact

- **Integration of Threat Intelligence** – The Threat Metrics group in CVSS v4.0 adjusts the severity of a vulnerability based on real-time factors, such as the availability of proof-of-concept code or active exploitation. This integration of threat intelligence ensures that the scoring reflects the current threat landscape and the likelihood of an attack
- **Environmental Metrics** – CVSS v4.0's Environmental Metrics further refine the severity score to a specific computing environment. They consider factors such as the presence of mitigations and the criticality of the affected system within the user's environment, allowing for a more tailored risk assessment
- **Simplified Threat Metrics** – The Threat Metrics group, previously known as Temporal Metrics, has been simplified to focus on the most critical aspect of real-time vulnerability assessment—Exploit Maturity. This simplification helps users better understand the risk of vulnerabilities
- **Enhanced Clarity and Simplicity** – CVSS v4.0 aims to reduce ambiguities and inconsistencies in vulnerability assessments that were common in previous versions. The new version provides clearer metric guidance and definitions, which should lead to more consistent scoring
- **Support for Multiple Scores** – The new framework is designed to support multiple CVSS scores for the same vulnerability when it affects different platforms or operating systems, providing a more comprehensive assessment
- **Focus on Resiliency** – CVSS v4.0 introduces a renewed focus on resiliency, particularly in the early stages of an exploit, which is increasingly important for the security of operational technology (OT), industrial control systems (ICS), and the Internet of Things (IoT)
- **Vendor-Supplied Severity and Impact Scoring** – The framework now integrates vendor-supplied severity and impact scoring, accommodating a wider range of perspectives and aligning the scoring process more closely with real-world scenarios
- **Enhanced Fidelity in Vulnerability Assessment** – The objective behind CVSS v4.0 is to offer enhanced fidelity in vulnerability assessment for the industry and the public, incorporating various refinements to improve the accuracy of vulnerability scoring

IV. Finer-grained metrics in CVSS v4.0 & Scoring process

CVSS v4.0 introduces several finer-grained metrics to provide a more nuanced understanding of the technical characteristics of vulnerabilities. One of the key changes is a more granular breakdown of the Base Metrics, which includes new values for User Interaction, categorized as either Passive or Active. The User Interaction (UI) metric in CVSS v4.0 provides more granularity to the amount of interaction required. Additionally, CVSS v4.0 introduces a new Attack Requirement metric, which provides more granularity in capturing the prerequisite conditions enabling an attack.

CVSS v4.0 simplifies the scoring process in several ways. The Threat Metrics, previously known as Temporal Metrics, have been simplified and renamed to emphasize real-time vulnerability assessment. Remediation Level (RL) and Report Confidence (RC) have been retired, and Exploit "Code" Maturity has been renamed to Exploit Maturity (E). The Temporal Metrics have been simplified to help consumers better understand the risk of vulnerabilities. The scoring system in CVSS v4.0 is simpler and more flexible compared to previous versions, aiming to provide a universal framework for scoring different vulnerabilities.

V. List of Metrics

The Common Vulnerability Scoring System (CVSS) version 4.0 consists of four metric groups: Base, Threat, Environmental, and Supplemental.

The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. The Base Score is calculated using a specific formula that examines factors such as the vulnerability's impact on integrity, confidentiality, availability, exploitability, and scope.

The Threat metric group, previously known as the Temporal Metrics Group, provides additional context to the Base metrics. However, the Threat metrics do not significantly impact the final CVSS score.

The Environmental metric group represents the characteristics of a vulnerability that are unique to a user's environment. These metrics allow organizations to customize the CVSS scores based on their specific environment. However, the Environmental metrics are specified by users and do not directly impact the publicly visible CVSS scores, which are based solely on the Base Score.

The Supplemental metric group is a new addition in CVSS v4.0. It includes metrics that provide additional context, such as Automatable, Value Density, Recovery, Provider Urgency, and Vulnerability Response Effort. However, the Supplemental metrics are optional and do not have any impact on the final calculated CVSS score.

A. Base Metrics

The Base Metrics represent the intrinsic qualities of a vulnerability. They include:

- Attack Vector (AV)
- Attack Complexity (AC)
- Privileges Required (PR)
- User Interaction (UI)
- Scope (S)
- Impact Metrics: Vulnerable System Confidentiality (VC), Integrity (VI), Availability (VA), and Subsequent System(s) Confidentiality (SC), Integrity (SI), Availability (SA)

1) Purpose

The Base metric group represents the intrinsic qualities of a vulnerability that are constant over time. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics. The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited, while the Impact metrics reflect the direct consequences of a successful exploit. The Base metrics help determine the initial severity score for a vulnerability. In CVSS v3.1, the base metric group consisted of four main metrics: Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), and User Interaction (UI). CVSS 4.0 introduced a metric called the Attack Requirements (AT) to increase the granularity of the scoring system

2) Impact on Score

The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Threat and Environmental metrics. The Base score only reflects the technical severity of a vulnerability when considered in isolation. It's important to note that the Base score is only the starting point for building a full picture of the risk associated with a vulnerability.

3) Usage

The Base metric group is used to assess the fundamental qualities of a vulnerability that maintain their constancy over time. It is used to evaluate the severity of vulnerabilities and their impact on organizations without considering temporal or environmental factors

4) Calculation

The Base Metrics are divided into Exploitability Metrics and Impact Metrics. When these Base Metrics are assigned values by an analyst, they result in a score ranging from 0.0 to 10.0.

The CVSS v4.0 calculator, which is a reference implementation of the CVSS standard, can be used for generating scores based on the values of these metrics. The calculator applies the formula specified in the CVSS version 4.0 standard to produce the Base Score

5) Prioritizing vulnerabilities

Base metrics represent the intrinsic qualities of a vulnerability that are constant over time and across user environments. They include exploitability metrics (such as Attack Vector, Attack Complexity, Attack Requirement, Privileges Required, and User Interaction) and vulnerable system impact metrics (such as Confidentiality, Integrity, and Availability) and subsequent system impact metrics. The Base metrics produce a score ranging from 0 to 10, which reflects the technical severity of a vulnerability when considered in isolation. This score is essential when analyzing a vulnerability and helps in prioritizing vulnerabilities based on their inherent characteristics

B. Threat Metrics

The Threat Metrics, previously known as Temporal Metrics, adjust the severity of a vulnerability based on real-time factors. They include:

- Exploit Maturity (E)
- Remediation Level (RL)
- Report Confidence (RC)

1) Purpose

The purpose of the Threat metric group is to adjust the severity of a vulnerability based on factors such as the availability of proof-of-concept code or active exploitation. This group captures vulnerability characteristics related to a threat, which may change over time.

For example, it can capture information such as whether the vulnerability has been exploited or if there is any proof-of-concept exploit available. The values found in this metric group may change over time, reflecting the evolving threat landscape.

2) Impact on Score

The Threat metric group impacts the final CVSS score by adjusting the severity of a vulnerability based on the threat landscape. The absence of explicit Threat metric selections will still result in a score, but the inclusion of the “T” in the nomenclature is appropriate if any Threat metrics are used to adjust the score

3) Usage

The Threat metric group is used to refine the severity score of a vulnerability based on applicable threat intelligence. It is used in combination with the Base metric group, which represents the intrinsic qualities of a vulnerability that are constant over time, and the Environmental metric group, which represents the characteristics of a vulnerability that are unique to a specific computing environment.

4) Calculation

The Threat Metrics in the Common Vulnerability Scoring System (CVSS) version 4.0 adjust the severity of a vulnerability based on factors such as the availability of proof-of-concept code or active exploitation. These metrics reflect the characteristics of a vulnerability related to threat that may change over time.

In CVSS v4.0, the Threat Metrics replaced the Temporal Metrics from previous versions, resulting in clearer and simplified metrics. The Remediation Level (RL) and Report Confidence (RC) metrics, which were part of the Temporal Metrics in previous versions, have been removed in CVSS v4.0.

The values assigned to the Threat Metrics are used in the calculation of the final score, along with the Base and Environmental Metrics. If explicit Threat Metric values are not provided, default values that assume the highest severity are used.

The CVSS v4.0 calculator, which is a reference implementation of the CVSS standard, can be used for generating scores based on the values of these metrics. The calculator applies the formula specified in the CVSS version 4.0 standard to produce the final score, which includes the Threat Metrics.

5) Prioritizing vulnerabilities

Threat metrics, previously known as Temporal Metrics, adjust the severity of a vulnerability based on factors such as the availability of proof-of-concept code or active exploitation. These metrics reflect the characteristics of a vulnerability that change over time, such as whether the vulnerability has been exploited or if any proof-of-concept exploit exists. The values in this metric group may change over time, and they help in real-time vulnerability assessment. By considering the likelihood of exploitation and the potential impact of a successful attack, CVSS v4.0 aims to offer a more holistic and accurate assessment of vulnerabilities.

C. Environmental Metrics

The Environmental Metrics allow organizations to customize the CVSS scores based on their specific environment. They include:

- Modified Base metrics
- Collateral Damage Potential (CDP)
- 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)

1) Purpose

The Environmental Metric Group in CVSS v4.0 represents the characteristics of a vulnerability that are unique to a user's environment. It allows organizations to adjust the Base Score of a vulnerability to reflect its impact within their specific context. This group accounts for the presence of security controls that may mitigate some or all consequences of a vulnerability and the relative importance of a vulnerable system within a technology infrastructure.

2) Impact on Score

The Environmental Metrics enable analysts to customize the CVSS score with inputs regarding IT asset importance and the presence of mitigations, which can increase or decrease the severity of a vulnerability. These metrics are modifiers to the base metric group and are designed to account for aspects of an enterprise that might influence the severity of a vulnerability. . The Environmental Metric Group impacts the final CVSS score by allowing adjustments based on the specific environment where the vulnerability exists.

3) Usage

The Environmental Metric Group is used to tailor the CVSS score to an organization's unique environment, considering factors such as the importance of the affected IT asset and the effectiveness of existing security controls. These metrics are the modified equivalent of the Base Metrics and are specified by users to provide a more accurate assessment of the risk posed by a vulnerability in their specific operational context.

4) Calculation

The Environmental Metrics in the Common Vulnerability Scoring System (CVSS) version 4.0 are designed to adjust the Base Score of a vulnerability to reflect the impact within a specific organizational context. These metrics account for the protection goals of the affected system and the presence of security controls that mitigate vulnerability.

The Environmental Metrics are calculated by first determining the Modified Base Metrics, which are the Base Metrics adjusted for the presence of mitigations or compensating controls. The Security Requirements are used to indicate the importance of the affected IT asset to the organization, which can amplify or reduce the severity based on the asset's criticality. The Collateral Damage Potential metric reflects the potential for non-direct damage to the environment or entities beyond the IT asset.

The final Environmental Score is derived by combining the Modified Base Metrics with the Security Requirements and Collateral Damage Potential, using a formula specified in the CVSS v4.0 Specification Document. This score provides a more tailored assessment of the vulnerability's severity within the specific environment of the organization

5) Prioritizing vulnerabilities

Environmental metrics further refine the resulting severity score to a specific computing environment. They consider factors such as the presence of mitigations in that environment and the criticality of the systems. These metrics are specified by users and can lead to a disconnect between the score and the actual risk in the real world due to their subjective nature. However, they are crucial in providing a more precise assessment of vulnerabilities in a specific environment, thus enhancing vulnerability prioritization and risk management.

D. Supplemental Metrics

The Supplemental Metrics provide additional context and describe aspects of a vulnerability that are outside the core CVSS standard. They include:

- Automatable (A)
- Value Density (VD)
- Recovery (R)
- Provider Urgency (PU)
- Vulnerability Response Effort (VRE)

1) Purpose

The purpose of the Supplemental Metric Group is to provide users with contextual information that allows for a more nuanced understanding of vulnerabilities. These metrics offer valuable insights into extrinsic aspects of vulnerabilities, allowing consumers to delve deeper into specific contextual considerations. They are designed to provide a more complete understanding of vulnerabilities by describing and measuring additional extrinsic attributes

2) Impact on Score

Unlike core CVSS metrics, Supplemental metrics do not contribute to the calculation of CVSS scores. They do not have any impact on the final calculated CVSS score. Instead, they serve as supplementary information for a more nuanced vulnerability assessment. Organizations may then assign importance and/or effective impact of each metric, or set/combination of metrics, giving them more, less, or absolutely no effect on the final risk analysis

3) Usage

The usage of each metric within the Supplemental metric group is determined by the scoring consumer. This contextual information may be employed differently in each consumer’s environment. The information consumer can then use the values of these Supplemental Metrics to take additional actions if they so choose, applying locally significant importance to the metrics and values

4) Calculation

The Supplemental Metrics in the Common Vulnerability Scoring System (CVSS) version 4.0 are a new addition designed to provide additional context and describe extrinsic attributes of a vulnerability. These metrics are optional and do not contribute to the calculation of the final CVSS score. Instead, they serve as supplementary information for a more nuanced vulnerability assessment.

The usage and response plan of each metric within the Supplemental metric group is determined by the scoring consumer. This contextual information may be employed differently in each consumer's environment. Organizations may then assign importance and/or effective impact of each metric, or set/combination of metrics, giving them more, less, or absolutely no effect on the final risk analysis.

5) Prioritizing vulnerabilities

Supplemental metrics are a new addition in CVSS v4.0. They measure extrinsic attributes of a vulnerability and provide contextual information. These metrics do not affect the vulnerability score but can be used to inform the companies that purchase the products. They include concepts such as "Automatable," "Recovery," and "Mitigation Effort," which provide additional context for vulnerability and remediation teams

E. Differences

The Supplemental Metric Group is used to provide additional context and does not affect the CVSS score, whereas the Base, Threat, and Environmental Metric Groups contribute directly to the scoring process and are essential for calculating the severity of a vulnerability. The Supplemental Metric Group in CVSS v4.0 is distinct from the Base, Threat, and Environmental Metric Groups in several ways:

Supplemental Metric Group:

- **Purpose**: Provides additional context and describes extrinsic attributes of a vulnerability that are outside the core CVSS standard
- **Impact on Score**: The metrics in this group do not impact the final calculated CVSS score. They are optional and are used to convey additional information that may influence an organization's risk analysis and response plan
- **Usage**: The usage and response plan of each metric within the Supplemental Metric Group is determined by the scoring consumer, and this contextual information may be employed differently in each consumer's environment

Base, Threat, and Environmental Metric Groups:

- **Purpose**: These groups contain metrics that directly contribute to the calculation of the CVSS score, reflecting the intrinsic qualities of a vulnerability (Base), the real-time threat landscape (Threat), and the specific impact within an organizational context (Environmental)
- **Impact on Score**: The metrics in these groups directly affect the final CVSS score, with each group providing a different perspective on the severity and impact of the vulnerability
- **Usage**: The Base Metrics are provided by the organization maintaining the vulnerable system or a third party, while the Threat and Environmental Metrics are intended for end consumers to enrich the Base metrics with additional context

VI. Operational Technology Exposure Metrics in CVSS v4.0

In CVSS v4.0, new metrics have been introduced to address the exposure and impact of vulnerabilities in Operational Technology (OT). These metrics are particularly relevant due to the increasing concerns around the security of OT, industrial control systems (ICS), and the Internet of Things (IoT). The updates aim to provide a more accurate assessment of the risks associated with vulnerabilities in these environments

A. Safety Metrics

Safety metrics have been added to both the Supplemental and Environmental metric groups in CVSS v4.0. These metrics assess the potential safety impact of exploiting a vulnerability, which is especially important in sectors like healthcare or industrial control systems where safety is a critical concern

B. OT-Specific Considerations

The new metrics for Operational Technology exposure include considerations for whether the "consequences of the vulnerability meet the definition of IEC 61508," which is a standard for the functional safety of electrical/electronic/programmable electronic safety-related systems . This inclusion reflects the growing concern about OT cyber risk and the need for a scoring system that can adequately capture the unique risks associated with OT environments

C. Impact on Vulnerable and Subsequent Systems

CVSS v4.0 also emphasizes evaluating the impact of vulnerability exploitation on both the vulnerable system and subsequent systems. This is particularly relevant for OT environments where a vulnerability in one component could potentially have cascading effects on other interconnected systems

D. Use of Supplemental and Environmental Metrics

While the Supplemental metrics do not directly impact the final CVSS score, they provide valuable contextual information that can be used by organizations to inform their risk analysis and response plans. The Environmental metrics allow for customization of the CVSS scores based on the specific environment, which can include OT settings

References

[1] First, "Common Vulnerability Scoring System", https://www.first.org/cvss/v4-0/, Accessed: Mar 8th, 2024