Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is an industry standard for calculating the severity ratings of vulnerabilities. This guide provides an overview of how CVSS scores are derived, as well as an introduction to Microsoft DREAD, a risk assessment system that complements CVSS.

Microsoft DREAD

DREAD is a risk assessment model developed by Microsoft to evaluate the severity of security threats and vulnerabilities. The model uses a scale of 10 points to assess the risk based on five factors:

1. Damage Potential: The potential damage caused by the threat.
2. Reproducibility: The ease of reproducing the attack.
3. Exploitability: The ease of exploiting the vulnerability.
4. Affected Users: The number of users affected.
5. Discoverability: The likelihood of the threat being discovered.

CVSS Metric Groups

Base Metric Group

The CVSS Base Metric Group represents the intrinsic characteristics of a vulnerability.

Exploitability Metrics

Attack Vector (AV): Context by which vulnerability exploitation is possible.
Attack Complexity (AC): Conditions beyond the attacker's control that must exist.
Privileges Required (PR): Level of privileges an attacker must possess.
User Interaction (UI): Requirement for a user to participate in the successful exploitation.

Impact Metrics

The impact on the CIA triad (Confidentiality, Integrity, Availability) when a vulnerability is exploited.
Confidentiality Impact (C)
Integrity Impact (I)
Availability Impact (A)

Temporal Metric Group

These metrics measure the current state of exploit techniques, availability of patches, and the level of confidence in the vulnerability.

Exploit Code Maturity (E): Likelihood of the vulnerability being exploited.
Remediation Level (RL): The availability and type of a fix.
Report Confidence (RC): The degree of confidence in the existence and details of the vulnerability.

Environmental Metric Group

These metrics represent the characteristics of the vulnerability that are relevant and unique to a particular user's environment.

Modified Base Metrics: Adjusted metrics based on the specific environment’s impact on the CIA triad.

CVSS Calculation Example

For instance, the Windows Print Spooler Remote Code Execution Vulnerability has a CVSS Base Metric score of 8.8. The specific metric values can be referenced from the National Vulnerability Database.

Risk Scoring and Prioritization

CVSS scores help organizations categorize and prioritize vulnerabilities based on severity. Understanding these scores enables IT security professionals to justify and calculate scores manually when necessary.

For further details and a CVSS calculator, visit the National Vulnerability Database: https://nvd.nist.gov/vuln-metrics/cvss