Common Vulnerability Scoring System (CVSS)

Overview

There are various ways to score or calculate severity ratings of vulnerabilities. The Common Vulnerability Scoring System (CVSS) is an industry standard for performing these calculations. Many scanning tools will apply these scores to each finding as a part of the scan results, but it's important that we understand how these scores are derived in case we ever need to calculate one by hand or justify the score applied to a given vulnerability. The CVSS is often used together with the so-called Microsoft DREAD. DREAD is a risk assessment system developed by Microsoft to help IT security professionals evaluate the severity of security threats and vulnerabilities. It is used to perform a risk analysis by using a scale of 10 points to assess the severity of security threats and vulnerabilities. With this, we calculate the risk of a threat or vulnerability based on five main factors:

- Damage Potential
- Reproducibility
- Exploitability
- Affected Users
- Discoverability

The model is essential to Microsoft's security strategy and is used to monitor, assess, and respond to security threats and vulnerabilities in Microsoft products. It also serves as a reference for IT security professionals and managers to perform their risk assessment and prioritisation of security threats and vulnerabilities.

Risk Scoring

The CVSS system helps categorise the risk associated with an issue and allows organisations to prioritise issues based on the rating. The CVSS scoring consists of the exploitability and impact of an issue. The exploitability measurements consist of access vector, access complexity, and authentication. The impact metrics consist of the CIA triad, including confidentiality, integrity, and availability.

Base Metric Group

The CVSS base metric group represents the vulnerability characteristics and consists of exploitability metrics and impact metrics.

Exploitability Metrics
The Exploitability metrics are a way to evaluate the technical means needed to exploit the issue using the metrics below:

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

Impact Metrics
The Impact metrics represent the repercussions of successfully exploiting an issue and what is impacted in an environment, and it is based on the CIA triad. The CIA triad is an acronym for Confidentiality, Integrity, and Availability.

CIA Triad

Confidentiality Impact relates to securing information and ensuring only authorised individuals have access. For example, a high severity value would be in the case of an attacker stealing passwords or encryption keys. A low severity value would relate to an attacker taking information that may not be a vital asset to an organisation.

Integrity Impact relates to information not being changed or tampered with to maintain accuracy. For example, a high severity would be if an attacker modified crucial business files in an organisation's environment. A low severity value would be if an attacker could not specifically control the number of changed or modified files.

Availability Impact relates to having information readily attainable for business requirements. For example, a high value would be if an attacker caused an environment to be completely unavailable for business. A low value would be if an attacker could not entirely deny access to business assets and users could still access some organisation assets.

Temporal Metric Group

The Temporal Metric Group details the availability of exploits or patches regarding the issue.

Exploit Code Maturity
The Exploit Code Maturity metric represents the probability of an issue being exploited based on ease of exploitation techniques. There are various metric values associated with this metric, including Not Defined, High, Functional, Proof-of-Concept, and Unproven.

- A 'Not Defined' value relates to skipping this particular metric.
- A 'High' value represents an exploit consistently working for the issue and is easily identifiable with automated tools.
- A 'Functional' value indicates there is exploit code available to the public.
- A 'Proof-of-Concept' demonstrates that a PoC exploit code is available but would require changes for an attacker to exploit the issue successfully.

Remediation Level
The Remediation level is used to identify the prioritisation of a vulnerability. The metric values associated with this metric include Not Defined, Unavailable, Workaround, Temporary Fix, and Official Fix.

- A 'Not Defined' value relates to skipping this particular metric.
- An 'Unavailable' value indicates there is no patch available for the vulnerability.
- A 'Workaround' value indicates an unofficial solution released until an official patch by the vendor.
- A 'Temporary Fix' means an official vendor has provided a temporary solution but has not released a patch yet for the issue.

- An 'Official Fix' indicates a vendor has released an official patch for the issue for the public.

Report Confidence
Report Confidence represents the validation of the vulnerability and how accurate the technical details of the issue are. The metric values associated with this metric include Not Defined, Confirmed, Reasonable, and Unknown.

- A 'Not Defined' value relates to skipping this particular metric.
- A 'Confirmed' value indicates there are various sources with detailed information confirming the vulnerability.
- A 'Reasonable' value indicates sources have published information about the vulnerability. However, there is no complete confidence that someone would achieve the same result due to missing details of reproducing the exploit for the issue.

Environmental Metric Group

The Environmental metric group represents the significance of the vulnerability of an organisation, taking into account the CIA triad.

Modified Base Metrics
The Modified Base metrics represent the metrics that can be altered if the affected organisation deems a more significant risk in Confidentiality, Integrity, and Availability to their organisation. The values associated with this metric are Not Defined, High, Medium, and Low.

- A 'Not Defined' value would indicate skipping this metric.
- A 'High' value would mean one of the elements of the CIA triad would have astronomical effects on the overall organisation and customers.
- A 'Medium' value would indicate one of the elements of the CIA triad would have significant effects on the overall organisation and customers.
- A 'Low' value would mean one of the elements of the CIA triad would have minimal effects on the overall organisation and customers.

Calculating CVSS Severity

The calculation of a CVSS v3.1 score takes into account all the metrics discussed in this section. The National Vulnerability Database has a calculator available to the public here.

CVSS Calculation Example
For example, for the Windows Print Spooler Remote Code Execution Vulnerability, CVSS Base Metrics is 8.8. You can reference the values of each metric value here.