Apexa IQ Day 10

*National Vulnerability Database (NVD):*

*The* ***National Vulnerability Database (NVD)*** *is a publicly available repository of information on security vulnerabilities. It is managed by the* ***National Institute of Standards and Technology (NIST)*** *under the U.S. Department of Commerce. The database serves as a central resource* ***for security professionals, researchers, and organizations to track, assess, and mitigate cybersecurity risks.***

*The NVD provides* ***standardized information*** *on vulnerabilities, including severity ratings, impact metrics, and links to mitigation strategies. It is primarily based on the* ***Common Vulnerabilities and Exposures (CVE) system****, meaning each entry in the NVD corresponds to a specific CVE identifier.*

*There are some terminologies are associated with NVD, these are given below:*

1. *Common Vulnerabilities and Exposures:*

*Common Vulnerabilities and Exposures (CVE) is a publicly accessible database that* ***identifies and catalogs known security vulnerabilities in software and hardware****, assigning each vulnerability* ***a unique identifier*** *to facilitate information sharing and prioritization of fixes; essentially, CVE is the core data source used by NVD to list vulnerabilities.*

1. *CVSS:*

*CVSS stands for* ***Common Vulnerability Scoring System*** *and with the help of this NVD assigns* ***a severity score*** *helping organization prioritize their vulnerabilities.*

1. *Common Platform Enumeration:*

***Common Platform Enumeration*** *(CPE) is standardized way of* ***naming and identifying software products****, allowing for a specific identification of* ***specific versions*** *of systems when discussing vulnerabilities within the NVD database.*

1. *CWE:*

*CWE stands for* ***Common Weakness Enumeration****, which is a categorized list of common* ***software and hardware weaknesses*** *that can potentially lead to security vulnerabilities, allowing analysts to classify the root cause of a vulnerability within a CVE entry by linking it to a specific CWE identifier.*

*Working of NVD:*

1. ***Data Collection***

* *The NVD ingests vulnerability data primarily from the* ***CVE list****, managed by MITRE Corporation.*
* *Vendors, researchers, and organizations submit vulnerability reports to the CVE system.*

1. ***Analysis and Scoring***

* *NVD analysts enrich the data by assigning* ***CVSS scores****, mapping vulnerabilities to* ***CWE categories****, and linking relevant security advisories.*

1. ***Publication and Updates***

* *Once validated, the vulnerabilities are published in the NVD, making them accessible via search, RSS feeds, and API integrations.*

1. ***Integration with Security Tools***

* *Many cybersecurity tools (e.g., vulnerability scanners, SIEMs) integrate with NVD to enhance security monitoring.*

*What Scoring Information is Provided for Each Vulnerability?*

*The*[*Common Vulnerability Scoring System*](https://nvd.nist.gov/vuln-metrics/cvss)*(CVSS) is an open set of standards used to assess a vulnerability and assign a severity on a scale of 0 to 10. The NVD provides CVSS ‘base scores’ which represent the innate characteristics of each vulnerability. The severity ratings as per CVSS v3.0 specifications are:*

|  |  |
| --- | --- |
| ***Severity*** | ***Base Score*** |
| *None* | *0.0* |
| *Low* | *0.1 – 3.9* |
| *Medium* | *4.0 – 6.9* |
| *High* | *7.0 – 8.9* |
| *Critical* | *9.0 – 10* |

*What Is the Difference Between NVD and CVE?*

*While these two lists/databases are often talked about interchangeably, they are actually separate, though interconnected, entities. CVE is essentially a list of vulnerability entries and NVD is a more robust database that is built upon and fully synchronized with the CVE list so that any updates made to the CVE list appear in the NVD. The NVD also adds the analysis component for each vulnerability, as described above.*[*As per MITRE*](https://cve.mitre.org/about/cve_and_nvd_relationship.html#:~:text=CVE%20%2D%20A%20list%20of%20entries,for%20publicly%20known%20cybersecurity%20vulnerabilities.&text=NVD%20%2D%20A%20vulnerability%20database%20built,CVE%20appear%20immediately%20in%20NVD.)*, the CVE list feeds the NVD. The U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (DHS CISA) sponsors both.*

*Importance of NVD*

* ***Risk Assessment & Management****: Helps organizations assess cybersecurity risks and prioritize mitigation efforts.*
* ***Automation & Integration****: Security tools use NVD data to automate vulnerability detection and response.*
* ***Compliance & Regulations****: Supports compliance with standards like* ***NIST 800-53, ISO 27001, and PCI DSS****.*
* ***Threat Intelligence****: Enables researchers and security teams to analyse trends and attack patterns.*

*How to Use NVD*

* ***Access the database****: Visit* [*NVD Website*](https://nvd.nist.gov/)*.*
* ***Search vulnerabilities****: Use keywords, CVE IDs, or filters.*
* ***Monitor RSS (Really Simple Syndication) feeds****: Stay updated on new vulnerabilities.*
* ***Integrate with security tools****: Use APIs for automated scanning.*