APEXAIQ Assignment | date:14/02/2025

**What is NVD?**

NVD is a platform in which we can search and find vulnerabilities of any Vendor.

With the help of this platform you can fix bugs in your software, hardware and in network also.

**We can find vulnerabilities with the help of NVD Platform link URL**: <https://nvd.nist.gov>

**1. National Vulnerability Database (NVD)**

* **Definition**: The **NVD** is a public, U.S. government-managed repository of cybersecurity vulnerabilities. It provides information on known security threats, categorized by severity, impact, and mitigation strategies.
* **Managed by**: The **National Institute of Standards and Technology (NIST)**.
* **Purpose**: Supports security teams by providing a standardized method for assessing and responding to vulnerabilities.
* **Data Sources**: NVD derives its information from **CVE**, adds impact metrics (CVSS scores), and includes remediation steps.

**NVD for Software**

* Contains vulnerabilities related to **operating systems, applications, and programming frameworks**.
* Helps developers identify security weaknesses in software libraries.
* **Example:** A zero-day vulnerability in **Apache Log4j (CVE-2021-44228)** is documented in NVD with severity ratings and mitigation steps.

**NVD for Hardware**

* Tracks vulnerabilities in **processors, firmware, IoT devices, and embedded systems**.
* Provides details on **hardware**-related security **risks** like **Meltdown and Spectre (CVE-2017-5753, CVE-2017-5715)**, which **affect modern CPUs**.
* Assists hardware manufacturers in developing **security patches**.

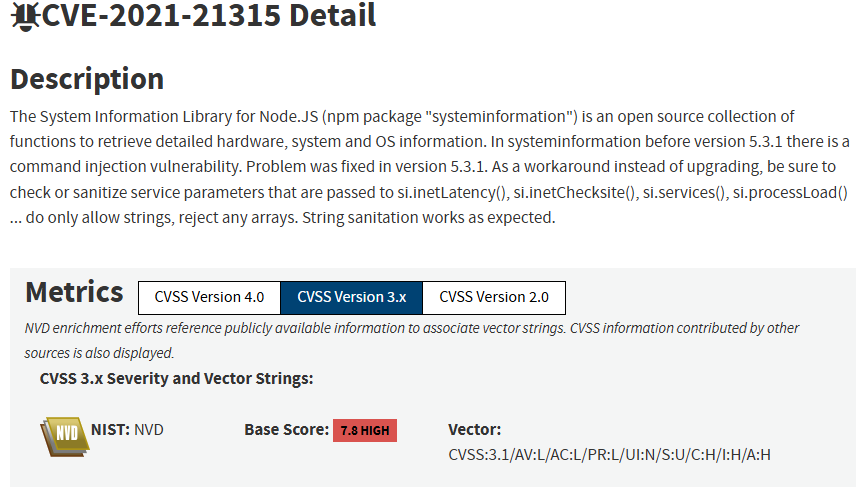
**NVD for Network**

* Includes vulnerabilities in **routers, firewalls, VPNs, and network protocols**.
* Helps network administrators assess risk and apply security updates.
* Example: **CVE-2019-0708 ("BlueKeep")**, a vulnerability in **Remote Desktop Protocol (RDP)**, is listed in NVD with mitigation strategies.

**p2. Common Vulnerabilities and Exposures (CVE)**

* **Definition**: **CVE** is a system that assigns a unique identifier to known cybersecurity vulnerabilities.
* **Managed by**: The **MITRE Corporation**.
* **Purpose**: Provides a standardized way to identify and track vulnerabilities across different vendors and platforms.

**Example**



**CVE for Software**

* Used by security tools to detect software flaws in **applications, operating systems, and libraries**.
* Helps software developers and security teams prioritize fixes.
* Example: **CVE-2020-1472 (Zerologon)** allowed privilege escalation in **Windows Server Netlogon**.

**CVE for Hardware**

* Identifies flaws in **microprocessors, firmware, and hardware components**.
* Security researchers use CVEs to report hardware vulnerabilities.
* Example: **CVE-2018-3646** affects **Intel CPUs**, allowing **side-channel attacks**.

**CVE for Network**

* Catalogs vulnerabilities in **network appliances, protocols, and services**.
* Helps IT teams secure network infrastructure.
* Example: **CVE-2023-23397**, a **Microsoft Outlook vulnerability**, allowed attackers to steal **NTLM hashes** remotely.

**Key Differences: NVD vs. CVE**

| **Feature** | **NVD** | **CVE** |
| --- | --- | --- |
| **Purpose** | A comprehensive database with vulnerability details, CVSS scores, and mitigation steps | A list of unique identifiers for security vulnerabilities |
| **Managed by** | NIST (National Institute of Standards and Technology) | MITRE Corporation |
| **Scope** | **Provides detailed descriptions, severity analysis, and remediation guides** | **Only assigns an ID and brief description** |
| **Usage** | Used by security professionals for risk assessment and patch management | Used as a reference in vulnerability scanning and reports |

**Conclusion**

* **NVD** provides a **detailed** analysis of vulnerabilities, including severity scoring (CVSS) and fixes.
* **CVE** acts as a **catalog of unique identifiers** for vulnerabilities, making it easier to track and reference threats.
* Both are **essential tools** for managing cybersecurity risks across **software, hardware, and networks**.

**3. Common Platform Enumeration (CPE):**

* Known Affected Software Configuration
* CPE identifiers are commonly used to **search** for **Common Vulnerabilities and Exposures** (CVEs) that affect the identified **product**.
* Is a **structured naming** scheme for information technology systems, software, and packages.
* **Example:-** **NVD :**- The value of CPE Name Matching is in determining if a particular product is **installed** on a system.
* Suppose that an **organization** is identifying which of its **systems** have any variation of **Microsoft Internet Explorer 8 installed**. This could be represented with the following well-formed CPE name (WFN):

wfn:[part="a",vendor="microsoft",product="internet\_explorer",  
version="8\.\*",update=ANY,edition=ANY,language=ANY] An **asset** management tool could collect information on the software installed on a system and compare its Internet Explorer installation characteristics to the WFN above. Suppose that the WFN for a particular installed instance of Internet Explorer was reported as: wfn:[part="a",vendor="microsoft",product="internet\_explorer",  
version="8\.0\.6001",update=NA,edition=NA,language="en\-us"]

**CPE are by default that are 2.2 and 2.3 as Unique Identification Name**

**CPE is only one and multiple CVE**

**4.CVSS Range (Common Vulnerability Scoring System):-**

* Severity Levels for Security Issues
* This severity level is based on self-calculated CVSS score for each specific vulnerability.

|  |  |  |
| --- | --- | --- |
| **CVSS SCORE RANGE** |  | **SEVERITY IN ADVISORY** |
| **9.0 - 10.0** |  | **Critical** |
| **7.0 - 8.9** |  | **High** |
| **4.0 - 6.9** |  | **Medium** |
| **0.1 - 3.9** |  | **Low** |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **How to Use the API**

1. **Make API Calls** to search for vulnerabilities using programming languages like Python.
2. **Example Python Script** to search for vulnerabilities:

With python language :-

import requests

base\_url = "https://services.nvd.nist.gov/rest/json/cves/1.0"

query = {"keyword": "Windows RDP"} # Replace with your search term

response = requests.get(base\_url, params=query)

data = response.json()

print(data)