University of Dhaka
Dept. of Computer Science and Engineering
Professional Masters in Information and Cyber Security (PMICS) Program

CSE 808 - Information Infrastructure Protection

“CVE: Common Vulnerabilities and Exposures”

Lab Class 4 – Manual

Conducted by: Md. Shakhawat Hossain Robin

What is CVE?

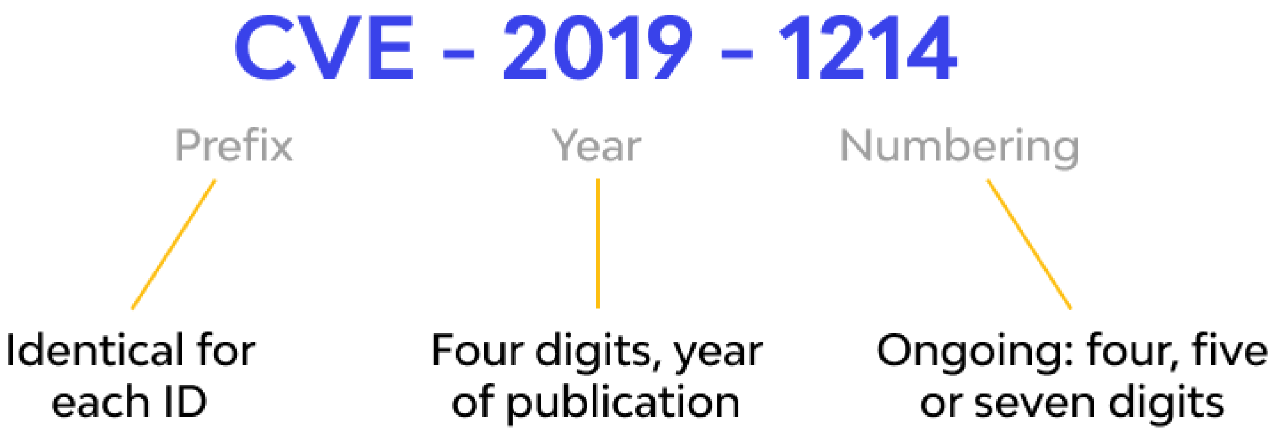
- The CVE program was initiated in the late 1990s by the cybersecurity community to address the growing need for a standardized approach to identifying and tracking vulnerabilities.
- CVE stands for Common Vulnerabilities and Exposures which provides a common language for discussing and sharing information about security vulnerabilities across different organizations and industries.
- It is a standardized system for uniquely identifying and tracking cybersecurity vulnerabilities in software and hardware products.

Importance of CVE

- **Standardization:** CVE provides a standardized naming scheme for vulnerabilities, making it easier for security professionals to communicate and share information about vulnerabilities.
- **Awareness:** CVE helps raise awareness about cybersecurity vulnerabilities by providing a common reference point for discussing and tracking them.
- **Prioritization:** CVE allows organizations to prioritize their response to vulnerabilities based on severity and impact.
- **Coordination:** CVE facilitates collaboration among security researchers, vendors, and organizations by providing a centralized repository of vulnerability information.
- **Patch Management:** CVE assists in the management and deployment of security patches by providing a clear reference to the vulnerabilities being addressed.
- **Compliance:** Many cybersecurity regulations and standards require organizations to track and address CVEs as part of their security programs.

CVE Identifiers

When vulnerabilities are verified, a CVE Numbering Authority (CNA) assigns a number. A CVE identifier follows the format of — CVE-{year}-{ID}. There are currently 114 organizations, across 22 countries, that are certified as CNAs. These organizations include research organizations, and security and IT vendors. CNAs are granted their authority by MITRE, which can also assign CVE numbers directly.


CVE - 2019 - 1214
Prefix
Year
Numbering
Identical for each ID
Four digits, year of publication
Ongoing: four, five or seven digits

Process of CVE analysis

Identification of vulnerabilities

- **Vulnerability Discovery:** Security researchers, vendors, and users discover vulnerabilities through various means such as penetration testing, bug bounty programs, and incident reports.
- **Vulnerability Assessment:** Vulnerabilities are assessed to determine their severity, impact, and potential risk to affected systems.
- **Vulnerability Classification:** Vulnerabilities are categorized based on their type, affected software/hardware, and potential attack vectors.

Process of CVE analysis

Assignment of CVE IDs

- **Request Submission:** Individuals or organizations submit requests for CVE IDs to a designated CVE Numbering Authority (CNA) or directly to the MITRE Corporation, the primary CVE authority.
- **Verification:** The CVE ID request is verified to ensure that the reported vulnerability meets the criteria for CVE assignment.
- **Assignment:** Once verified, a unique CVE ID is assigned to the vulnerability.
- **Public Disclosure:** The assigned CVE ID is publicly disclosed along with relevant details about the vulnerability in the CVE database and other security repositories.

Process of CVE analysis

Collaboration and Review

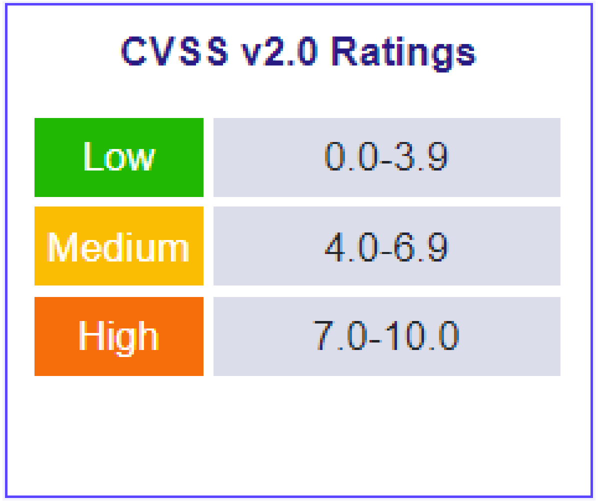
- **Collaboration:** Security researchers, vendors, and CNAs collaborate to ensure accurate and comprehensive coverage of vulnerabilities.
- **Peer Review:** CVE entries undergo peer review by the community to validate the accuracy and relevance of the information provided.

Role of CVE in Vulnerability Management

- **Identification:** CVE serves as a key component in the identification and tracking of vulnerabilities across software and hardware products.
- **Prioritization:** CVE helps organizations prioritize their response to vulnerabilities based on severity ratings and other factors.
- **Coordination:** CVE facilitates coordination among security researchers, vendors, and organizations in the management and mitigation of vulnerabilities.
- **Patch Management:** CVE assists in patch management by providing a clear reference to the vulnerabilities being addressed in software updates and security patches.
- **Incident Response:** CVE supports incident response efforts by providing timely information about known vulnerabilities and potential threats.

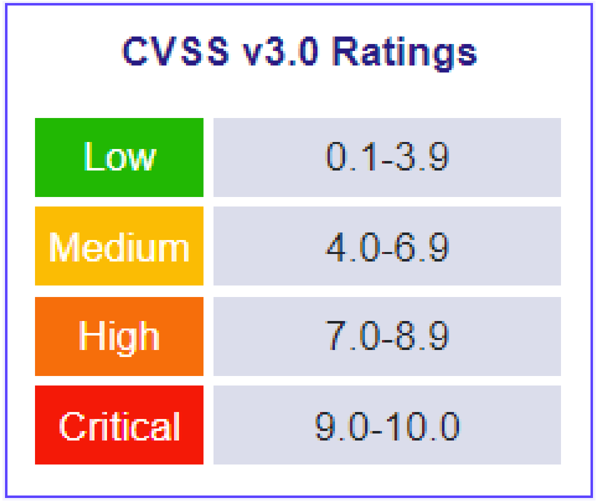
Common Vulnerability Scoring System (CVSS)

The CVSS is one of several ways to measure the impact of vulnerabilities, which is commonly known as the CVE score. The CVSS is an open set of standards used to assess a vulnerability and assign a severity along a scale of 0-10. The current version of CVSS is v3.1, which breaks down the scale is as follows:



CVSS v2.0 Ratings

Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0



CVSS v3.0 Ratings

Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVE Database

- The CVE database is a centralized repository of cybersecurity vulnerabilities tracked and documented using Common Vulnerabilities and Exposures (CVE) IDs.
- It contains detailed information about known vulnerabilities, including descriptions, affected products, severity ratings, and references to additional resources.
- The CVE database serves as a valuable resource for security professionals, providing a comprehensive and standardized reference for vulnerability management and mitigation efforts.

CVE Database (Links)

CVE Website: The official website of the CVE program, managed by the MITRE Corporation.

- https://www.cve.org/
- https://cve.mitre.org

CVE Details is a third-party platform that aggregates CVE data and provides statistics, charts, graphs, etc.

- https://www.cvedetails.com/

The NVD is a U.S. government repository that includes CVE data vulnerability metrics, impact scores, etc.

- https://nvd.nist.gov/

VULDB is a community-driven vulnerability database, provides information on vulnerability management, incident response, and threat intelligence.

- https://vuldb.com/

CVE GitHub Repository contains tools, scripts, JSON files and schema.related to the CVE program

- https://github.com/CVEProject/cvelist

The CVE Blog features articles, announcements, and insights related to CVE, including CVE assignments, vulnerability trends, and program updates.

- https://cve.mitre.org/blog

Thanks to all