# UNIT 3

## Unit 3: Standards - Common Vulnerabilities and Exposure, Common Vulnerability Scoring System, - National Vulnerability Database(NVD) - Common Platform Enumeration - Security Content Automation Protocol - Trusted Automated exchange of indicator information - OWASP Application security verification standard - Payment Card Industry - PCI compliance - HIPAA - HIPAA compliance

What is a cybersecurity standard?

A cybersecurity standard is a set of guidelines or best practices that organizations can use to improve their cybersecurity posture.

Organizations can use cybersecurity standards to help them identify and implement appropriate measures to protect their systems and data from cyber threats. Standards can also provide guidance on how to respond to and recover from cybersecurity incidents.

Here's a list of popular assessment standards:

- NIST (National Institute of Standards and Technology)
- CIS Controls (Center for Internet Security Controls)
- ISO (International Organization for Standardization)
- HIPAA (Health Insurance Portability and Accountability Act) / HITECH Omnibus Rule
- PCI-DSS (The Payment Card Industry Data Security Standard)
- GDPR (General Data Protection Regulation)
- CCPA (California Consumer Privacy Act)
- AICPA (American Institute of Certified Public Accountants)
- SOX (Sarbanes-Oxley Act)
- COBIT (Control Objectives for Information and Related Technologies)

- GLBA (Gramm-Leach-Bliley Act)
- FISMA (Federal Information Security Modernization Act of 2014)

**DFARS (Defense Federal Acquisition Regulation Supplement)**

The DFARS (Defense Federal Acquisition Regulation Supplement) is a set of regulations issued by the DOD (Department of Defense) that supplements the Federal Acquisition Regulation. The DFARS provides guidance and procedures for acquiring supplies and services for the DOD.

DOD government acquisition officials, contractors, and subcontractors doing business with the DOD must adhere to the DFARS.

**HIPAA (Health Insurance Portability and Accountability Act)**

The HIPAA (Health Insurance Portability and Accountability Act) is a set of federal regulations that protect the privacy of patients' health information. The HIPAA applies to all forms of health information, including paper records, electronic records, and oral communications.

It aims to make it easier for people to keep their health insurance when they change jobs, protect the confidentiality and security of health care information, and help the health care industry control its administrative costs.

**ISO 22301**

ISO 22301 is an international standard that outlines how organizations can ensure business continuity and protect themselves from disaster. The Standard provides a framework for a comprehensive BCMS (business continuity management system). It can be used by any organization, regardless of size, industry, or location.

**ISO/IEC 27001**

ISO 27001 is an international standard for information security that provides a framework for managing sensitive company information. The Standard includes

requirements for developing an ISMS (information security management system), implementing security controls, and conducting risk assessments.

The Standard's framework is designed to help organizations manage their security practices in one place, consistently and cost-effectively.

## ISO/IEC 27002

ISO 27002 is the code of practice for information security management. It provides guidance and recommendations on how to implement security controls within an organization. ISO 27002 supports the ISO 27001 standard, which provides the requirements for an ISMS.

## NIST CSF (Cybersecurity Framework)

The NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is a voluntary framework that provides a set of standards, guidelines, and best practices for managing cybersecurity risks.

The framework helps organizations to identify, assess, and manage their cybersecurity risks in a structured and repeatable manner. The framework is not mandatory, but it is increasingly being adopted by organizations as a voluntary measure to improve their cybersecurity posture.

### CVE

The Common Vulnerabilities and Exposures (CVE) program is a dictionary or glossary of vulnerabilities that have been identified for specific code bases, such as software applications or open libraries.

### CVE Numbering Authorities (CNAs)

CNAs are organizations throughout the world that are also CVE program partners. CNAs are usually part of major corporations — such as Microsoft, Oracle or Apple — and they're

essentially a bridge between individuals who find a new vulnerability and the CVE community. They help the discovery process by checking and submitting documents about the vulnerability and publishing the CVE.

CNAs are also in charge of assigning unique IDs to new CVEs. The ID helps you find all the relevant information about a vulnerability or exposure. Different CVE databases worldwide use these IDs to add more detailed information about the CVE, including:

- Severity
- Affected software systems
- The steps to follow to patch the vulnerability and contain the damage

**What Is the Common Vulnerability Scoring System (CVSS)?**

CVSS is a numbering system for assigning priority and severity levels to CVEs. It works by assigning a number between 0.0 and 10.0 to a CVE, indicating its severity. A vulnerability with a CVSS score between 9.0 and 10.0 is considered critical and needs immediate action.

CVSS helps companies plan risk management and response strategies and prioritize their patching cycles. Many security advisories release lists of CVEs ordered by the CVSS scores, with more severe vulnerabilities at the top of the list.

**Qualitative Severity Ratings**

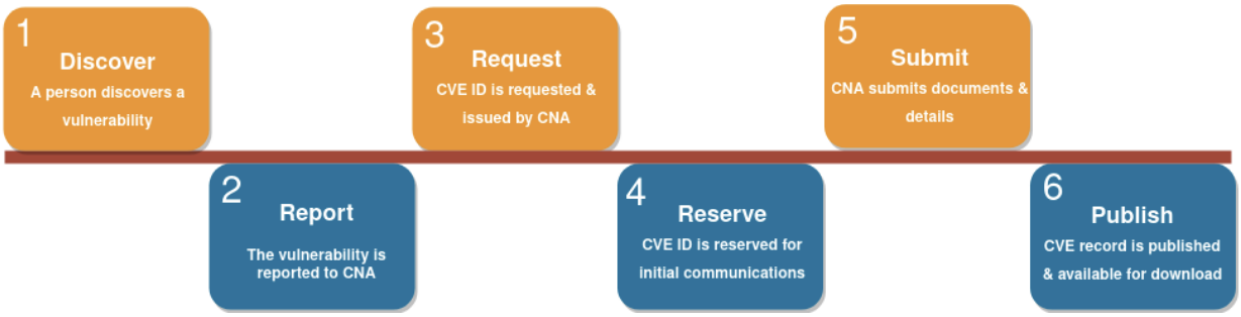
| CVSS v2.0 Ratings | | CVSS v3.x Ratings | | CVSS v4.0 Ratings | |
|---|---|---|---|---|---|
| **Severity** | **Severity Score Range** | **Severity** | **Severity Score Range** | **Severity** | **Severity Score Range** |
| | | None* | 0.0 | None* | 0.0 |

| | | | | | |
|---|---|---|---|---|---|
| Low | 0.0-3.9 | Low | 0.1-3.9 | Low | 0.1-3.9 |
| Medium | 4.0-6.9 | Medium | 4.0-6.9 | Medium | 4.0-6.9 |
| High | 7.0-10.0 | High | 7.0-8.9 | High | 7.0-8.9 |
| | | Critical | 9.0-10.0 | Critical | 9.0-10.0 |

The NVD notates qualitative severity ratings of "Low", "Medium", and "High" for CVSS v2.0 base score ranges in addition to the qualitative severity ratings for CVSS v3.x and CVSS v4.0 as they are defined in their respective specifications.

**CVE Lifecycle**

When a vulnerability is discovered, it must go through a standardized CVE lifecycle before publication. The image below shows a simplified flow.




**Discover**: The process starts with a person or organization discovering a vulnerability.

**Report**: The person or entity that discovered the vulnerability files a report with a CVE program partner.

**Request**: The CVE partner (CNA) issues an ID for the vulnerability.

**Reserve**: The ID is reserved for that particular vulnerability and is used in the early-stage assessment of the CVE and all related communications between different parties.

**Submit**: The CVE partner assesses the vulnerabilities submitted documents which should include all information needed to prove the presence of the vulnerability or exposure, the root cause, the type of threat and the impact.

**Publish**: After all the documented details are verified, the CNA publishes the CVE, making it public.

**NVD**

The National Vulnerability Database (NVD) is a U.S. government repository of standards-based vulnerability management data. It provides information about vulnerabilities in various software and hardware systems, helping organizations and individuals understand potential security risks and how to address them.

**Common Platform Enumeration (CPE) Dictionary**

CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

An example is the following name representing Microsoft Internet Explorer 8.0.6001 Beta:

wfn:[part="a",vendor="microsoft",product="internet_explorer",
version="8\.0\.6001",update="beta"]

This method of naming is known as a well-formed CPE name (WFN). It is an abstract logical construction. The CPE Naming specification defines procedures for binding WFNs to machine-readable encodings, as well as unbinding those encodings back to WFNs. One of the bindings, called a Uniform Resource Identifier (URI) binding, is included in CPE version 2.3 for backward compatibility with CPE version 2.2 [CPE22].

The URI binding representation of the WFN above is:

cpe:/a:microsoft:internet_explorer:8.0.6001:beta

The second binding defined in CPE 2.3 is called a formatted string binding.

It has a somewhat different syntax than the URI binding, and it also supports additional product attributes. With the formatted string binding, the WFN above can be represented by the following.

cpe:2.3:a:microsoft:internet_explorer:8.0.6001:beta:*:*:*:*:* 😙

WFN attribute-value pair:

a. part

b. vendor

c. product

d. version

e. update

f. edition

g. language

h. sw_edition

i. target_sw

j. target_hw

k. other

Ref:CPE - Common Platform Enumeration: CPE Specifications (mitre.org)

**Common Platform Enumeration (CPE)** is a standardized system used to identify software applications, operating systems, and hardware components within an organization's IT infrastructure. As part of the **Security Content Automation**

**Protocol (SCAP)**, developed by the National Institute of Standards and Technology (NIST), CPE provides a uniform method to describe these resources, making it easier to track and assess vulnerabilities.

The CPE format follows this structure:

**cpe:/<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>**

### Breaking Down the CPE Structure:

- **<part>**: Defines the type of system. Possible values include:
  - a – Application
  - h – Hardware
  - o – Operating System
- **<vendor>**: Name of the company that created the product.
- **<product>**: Product name detected within the system.
- **<version>**: Product version number.
- **<update>**: Lists product updates.
- **<edition>**: Software edition (if applicable).
- **<language>**: The identified language of the product.

For example, consider the CPE entry for an Adobe Flash Player vulnerability:

**cpe:/a:adobe:airsdk%26_compiler:18.0.0.180**

This CPE string helps organizations identify and manage vulnerabilities specific to certain software versions and configurations.

# Benefits of Using CPE

1. **Standardized Naming Convention**: CPE provides a machine-readable format for naming IT systems and products, making it easier to track and manage them.

2. **Efficient Product Comparison**: CPE acts as a common identifier, facilitating easy comparison between different software and hardware components.
3. **Integration with Applicability Statements**: CPE enables the use of logical statements to define which products or versions are impacted by vulnerabilities.
4. **Improved Security Audits**: Organizations can streamline audits, enhance situation awareness, and ensure compliance with regulations by using consistent identifiers.

# What is CVE (Common Vulnerabilities and Exposures)?

**Common Vulnerabilities and Exposures (CVE)** refers to a list of publicly disclosed cybersecurity vulnerabilities. Each vulnerability in the CVE list has a unique identifier known as a **CVE ID**. This identifier helps security teams track, communicate, and address specific vulnerabilities in their systems.

The format of a CVE ID looks like this:

**CVE-YYYY-NNNN**

- **YYYY**: The year the CVE was disclosed.
- **NNNN**: A unique serial number.

## Example:

A vulnerability in the TrueConf Server, discovered in 2022, is labeled as:

**CVE-2022-46763**

# Benefits of CVE

1. **Simplified Vulnerability Tracking**: CVE IDs make it easy to track and reference known vulnerabilities.
2. **Cross-Platform Interoperability**: CVE allows organizations to compare the coverage and suitability of security products.
3. **Supports Proactive Cybersecurity**: By referencing CVE IDs, organizations can update their security strategies to address the most recent vulnerabilities.

==========

**SCAP** (Security Content Automation Protocol) is a suite of standards developed by NIST (National Institute of Standards and Technology) to automate the management of security vulnerabilities and compliance in information systems. It provides a standardized approach to gathering, analyzing, and responding to security-related information.

**Key Components of SCAP**

1. **CVE (Common Vulnerabilities and Exposures)**:
    - **Purpose**: Provides a standardized identifier for publicly known cybersecurity vulnerabilities and exposures.
    - **Example**: CVE-2024-1234 refers to a specific vulnerability in a piece of software.
2. **CPE (Common Platform Enumeration)**:
    - **Purpose**: Standardizes the naming of operating systems, applications, and hardware platforms to enable consistent identification.
    - **Example**: cpe:2.3:a:example:example_app:1.0:::::::* identifies a specific version of an application.
3. **CVSS (Common Vulnerability Scoring System)**:
    - **Purpose**: Provides a method for scoring the severity of vulnerabilities, helping prioritize remediation efforts.

- **Example**: CVSS score of 7.5 indicates a high-severity vulnerability.

4. **XCCDF (Extensible Configuration Checklist Description Format)**:
    - **Purpose**: Defines security configuration checklists in a standardized XML format to help automate the assessment of security configurations.
    - **Example**: XCCDF can be used to create checklists for verifying that a system adheres to security best practices.
5. **OVAL (Open Vulnerability and Assessment Language)**:
    - **Purpose**: Provides a standardized language for specifying system characteristics and assessing vulnerabilities and configuration issues.
    - **Example**: OVAL definitions can be used to automate the detection of vulnerabilities or compliance with security policies.
6. **ASCI (Asset Security Configuration Inventory)**:
    - **Purpose**: Helps in maintaining and managing information about the security configurations of assets.

**How SCAP Works**

7. **Data Collection**: SCAP-compatible tools collect data on system configurations, installed software, and known vulnerabilities.
8. **Assessment**: The collected data is compared against security checklists (XCCDF) and vulnerability definitions (OVAL) to assess compliance and identify potential issues.
9. **Reporting**: The results are used to generate reports that detail vulnerabilities, compliance status, and other security metrics.

**Benefits of SCAP**

- **Standardization**: Provides a common framework for security assessment and vulnerability management, making it easier to compare and integrate tools and processes.
- **Automation**: Facilitates the automated assessment of security configurations and vulnerabilities, improving efficiency and accuracy.
- **Consistency**: Ensures consistent reporting and scoring of vulnerabilities and compliance issues across different systems and environments.

**Tools and Resources**

Several tools and resources support SCAP, including:

- **OpenSCAP**: An open-source framework that provides tools for SCAP compliance, including scanning, reporting, and analysis.
- **Nessus**: A widely used vulnerability scanner that integrates with SCAP to automate vulnerability assessments.
- **Qualys**: Provides cloud-based security and compliance solutions that support SCAP standards.

==========