Marcos de referencia

MITRE

Organización sin ánimo de lucro encargada de registrar y publicar información relativa a vulnerabilidaddes y ataques conocidos dentro del ámbito de la seguridad

CWE

Common Weakness Enumeration. Es una clasificación de todas las vulnerabilidades por tipo, dirigida a desarrolladores y profesionales dedicados a la seguridad. Cada una de las debilidades o malas prácticas de programación registradas en el catálogo pueden dar lugar a una vulnerabilidad en el software final. Tipos de vulnerabilidades.

- Clases: Vulnerabilidad descrita de forma genérica, suelen ser independientes del lenguaje.
- Vulnerabilidad Base: Descrita de una forma genérica pero con suficiente detalle para poder inferir métodos de detección y prevención
- Variantes: Descrita de forma muy detallada
- Composiciones: Compoesto por 2 o más vulnerabilidades
- Vistas: subconjunto de elementos agrupados para mejorar la visualización dentro de la web del CWE
- Categoría: Agrupación de elementos que comparten las mismas características.

El CWE tiene un listado de las 25 vulnerabilidades más peligrosas. El CWE contiene cerca de 1000 tipos de vulnerabilidades.

CVE

Common Vulnerabilities and Exposures es una lista de volnerabilidades conocidas en programas y librerías. Esta web representa las vulnerabilidades concretas, no los tipos. Cada entrada en esta web explota uno o varios tipos de vulnerabilidades asociadas al CWE.

CNA

Entidades encargadas de asignar los identificadores CVE. CVE Numbering Authorities. Exiten varios tipos:

- MITRE: El CNA primario
- Algunas compañías que participan en el programa CNA pueden asignar CVE a sus productos.

NVD

National Vulnerability Database es un proyecto del gobierno de EEUU que se encarga de recopilar información sibre vulnerabolidades. Similar al CVE, pero ampliado.

CAPEC

Common Attack Pattern Enumeration and Clasification es un catalogo de patrones de ataque conocidos que se usan para explotar vulnerabilidades. Detallan:

- Breve descripción
- Pasos para realizar ataque
- Prerrequisitos necesarios
- Soluciones y mitigaciones.

Contiene en torno a 550 patrones de ataque conocidos.

CVSS

Common Vulnerability Scoring System es una métrica para determinar la criticidad o el impacto de las vulnerabilidades. El MITRE NO usa esta métrica. Gestionado por el Forum of Incident Response and Security Teams (FIRST) que es una confederación de equipos de respuesta a equipos informáticos. Para calcular la puntuación es necesario proporcionar cierta info sobre la vulnerabilidad, a partir dela cual se obtiene una puntuación numérica mediante el uso de un algoritmo.

Para calcular esta métrica se usan características base, características particulares de un entorno completo y características ambientales.

- Métrica base: Cualidades independientes del entorno y del tiempo. Vector de acceso: Local, LAN, remoto... Complejidad del ataque, privilegios necesarios, métricas de impacto sobre la confidencialidad, integridad y disponibilidad
- Métrica temporal (opcional): Características de la vulnerabilidad que varían con el tiempo. Explotabilidad, estado de la medida correctora, fiabilidad del informe sobre la vulnerabilidad
- Métrica de entorno: Características de la vulnerabilidad relacionadas con el entorno que sufre el problema. Por lo tanto no existe un valor universal para esta métrica.