En general, el reporte de vulnerabilidades utilizando el Sistema de Puntuación de Vulnerabilidad Común (CVSS) v4.0 involucra tanto al investigador o individuo que descubre la vulnerabilidad como a la empresa o entidad que es responsable de la seguridad del sistema afectado. Ambas partes pueden desempeñar roles en la evaluación y asignación de valores a las métricas básicas del CVSS v4.0.

1. **Investigador o individuo que descubre la vulnerabilidad:** La persona o equipo que descubre la vulnerabilidad puede proporcionar información sobre la naturaleza y el impacto de la vulnerabilidad en función de su investigación. Esto podría incluir detalles sobre cómo se descubrió la vulnerabilidad, cómo se explota, qué partes del sistema se ven afectadas y qué consecuencias potenciales podría tener. Esta información ayudará a determinar los valores para las métricas básicas, como el Vector de Ataque (AV) y el Impacto de la Confidencialidad (C).
2. **Empresa o entidad responsable del sistema afectado:** La organización dueña o responsable del sistema afectado por la vulnerabilidad también tiene un papel importante. Deben revisar la información proporcionada por el investigador y verificar la precisión de los detalles técnicos. Además, la organización puede proporcionar información sobre el entorno en el que opera el sistema, lo que podría afectar la asignación de valores para algunas métricas. Por ejemplo, la Métrica de Entorno (E) podría variar según las medidas de seguridad implementadas por la organización.

Métricas básicas y Suplementarias

Básicas

Métricas básicas: son rellenadas por el individuo o equipo que realiza el análisis de la vulnerabilidad. **Influye en la puntuación:** Sí **Obligatorio**: Sí

Vector de ataque

Influye en la puntuación: Sí

Obligatorio: Sí

Complejidad del ataque

Influye en la puntuación: Sí

Obligatorio: Sí

Requerimientos del ataque

Influye en la puntuación: Sí

Obligatorio: Sí

Privilegios necesarios

Influye en la puntuación: Sí

Obligatorio: Sí

Interacción de usuario

Influye en la puntuación: Sí

Obligatorio: Sí

Impacto en la confidencialidad

Influye en la puntuación: Sí

Obligatorio: Sí

Impacto en la integridad

Influye en la puntuación: Sí

Obligatorio: Sí

Impacto en la disponibilidad

Influye en la puntuación: Sí

Obligatorio: Sí

Métrica de impacto en el sistema vulnerable

Confidencialidad

Influye en la puntuación: Sí

Obligatorio: Sí

Integridad

Influye en la puntuación: Sí

Obligatorio: Sí

Disponibilidad

Influye en la puntuación: Sí

Obligatorio: Sí

Métrica de impacto en el sistema subsecuente

Confidencialidad

Influye en la puntuación: Sí

Obligatorio: Sí

Integridad

Influye en la puntuación: Sí

Obligatorio: Sí

Disponibilidad

Influye en la puntuación: Sí

Obligatorio: Sí

Suplementarias

Métricas suplementarias: son rellenadas por ambos individuos, el individuo o equipo que realiza el análisis de la vulnerabilidad y la empresa/organización que usted esté evaluando.

Influye en la puntuación: No

Obligatorio: No

Seguridad

-

Influye en la puntuación: No

Obligatorio: No

-

Automatización

Influye en la puntuación: No

Obligatorio: No

Recuperación

Influye en la puntuación: No

Obligatorio: No

Densidad del valor

Influye en la puntuación: No

Obligatorio: No

Esfuerzo de respuesta en la vulnerabilidad

Influye en la puntuación: No

Obligatorio: No

Urgencia del proveedor

Influye en la puntuación: No

Obligatorio: No

Métricas de amenaza y de entorno

Amenaza

***Métricas de amenaza*:** Las Métricas de Amenazas miden el estado actual de las técnicas de explotación o la disponibilidad de código. Se espera que cambien con el tiempo y a menudo necesitan actualizarse.

Influye en la puntuación: No

Obligatorio: -

- **Madurez del Exploit**

Influye en la puntuación: Sí

- **Obligatorio**: -

Entorno

Métricas del entorno: son rellenadas por ambos individuos, el individuo o equipo que realiza el análisis de la vulnerabilidad y la empresa/organización que usted esté evaluando.

Influye en la puntuación: Sí

Obligatorio: No

Métricas base y de seguridad modificadas

Influye en la puntuación: Sí

Obligatorio: No

Métricas de explotabilidad

Vector de ataque

Influye en la puntuación: Sí

Obligatorio: No

Complejidad del ataque

Influye en la puntuación: Sí

Obligatorio: No

Requerimientos del ataque

Influye en la puntuación: Sí

Obligatorio: No

Privilegios necesarios

Influye en la puntuación: Sí

Obligatorio: No

Interacción de usuario

Influye en la puntuación: Sí

Obligatorio: No

Métricas de impacto en el sistema vulnerable

Confidencialidad

Influye en la puntuación: Sí

Obligatorio: No

Integridad

Influye en la puntuación: Sí

Obligatorio: No

Disponibilidad

Influye en la puntuación: Sí

Obligatorio: No

Métricas de impacto en el sistema subsecuente

Confidencialidad

Influye en la puntuación: Sí

Obligatorio: No

Integridad

Influye en la puntuación: Sí

Obligatorio: No

Disponibilidad

Influye en la puntuación: Sí

Obligatorio: No

Requisitos de seguridad

Influye en la puntuación: Sí

Obligatorio: No

Requisitos de confidencialidad

Influye en la puntuación: Sí

Obligatorio: No

Requisitos de integridad

Influye en la puntuación: Sí

Obligatorio: No

Requisitos de disponibilidad

Influye en la puntuación: Sí

Obligatorio: No