Introducción

La ciberseguridad es cada vez más importante en el mundo digital actual. Saber cómo evitar que una vulnerabilidad provoque un aumento de las amenazas y ataques potenciales puede ayudar a los profesionales de la seguridad a mantener sus redes e infraestructuras seguras y protegidas.

¿Cómo se identifican las vulnerabilidades de seguridad y se evalúa su gravedad? ¿Cómo puede ayudar a identificar las amenazas que aprovechan esas vulnerabilidades antes de que surjan? ¿Cómo establecer prioridades para abordar las vulnerabilidades y colaborar entre disciplinas de seguridad para idear intervenciones?

Los ejemplos de este documento explorarán las respuestas a estas preguntas basándose en la puntuación común de vulnerabilidades (CVSS). CVSS puede ser un factor clave en la priorización de vulnerabilidades.

En este documento, emprenderás un viaje de aprendizaje en el que se te presentarán los conceptos que guían la identificación precisa de amenazas de ciberseguridad.

¿Qué son los CVSS?

CVSS es un estándar abierto e independiente del proveedor diseñado para:

Transmitir las características y la gravedad de una vulnerabilidad de seguridad de un producto

Proporcionar información sobre la prioridad y la urgencia de la respuesta

Conceptos sobre los CVSS

CVSS transmite información que puede utilizar para identificar posibles amenazas a la seguridad utilizando varias categorías. Estas métricas se combinan para producir una **puntuación base CVSS** y una **cadena de vectores**.

Métricas Básicas

Las métricas base reflejan la gravedad de una vulnerabilidad según sus características *intrínsecas, las cuales suelen ser constantes con el tiempo. Las métricas base asumen el impacto razonable en el peor caso en diferentes entornos implementados. Esta categoría suele ser completada por el proveedor.

* La palabra "intrínseco" se refiere a algo que es inherente, esencial o característico de algo en su naturaleza básica o fundamental. Entonces, cuando hablamos de "vulnerabilidad intrínseca",

nos referimos a características o aspectos fundamentales de un sistema, software o proceso que los hacen susceptibles a amenazas y riesgos de seguridad.

En el contexto de la ciberseguridad y las tecnologías de la información, una vulnerabilidad intrínseca se refiere a debilidades o fallos que están inherentemente presentes en el diseño, la arquitectura o el funcionamiento de un sistema. Estas vulnerabilidades no son causadas por factores externos, sino que son parte integral del sistema mismo. Algunos ejemplos de características de vulnerabilidad intrínseca podrían incluir:

1. **Diseño inseguro:** Si un sistema está diseñado sin tener en cuenta las mejores prácticas de seguridad, podría tener debilidades intrínsecas que podrían ser aprovechadas por atacantes.
2. **Codificación deficiente:** Errores de programación, como desbordamientos de búfer o falta de validación de entrada, pueden ser características intrínsecas que permiten a los atacantes explotar vulnerabilidades.
3. **Dependencias de software desactualizadas:** Utilizar componentes de software obsoletos o vulnerables como parte del sistema puede crear debilidades intrínsecas.
4. **Configuraciones por defecto inseguras:** Si un sistema se implementa con configuraciones predeterminadas que no son seguras, podría ser vulnerable desde su inicio.
5. **Falta de control de acceso:** Si un sistema carece de mecanismos de autenticación y control de acceso sólidos, puede tener vulnerabilidades intrínsecas relacionadas con la autorización no adecuada.
6. **Gestión inadecuada de datos sensibles:** Si un sistema almacena o maneja datos sensibles sin cifrado o medidas de protección adecuadas, está expuesto a riesgos intrínsecos.
7. **Falta de actualizaciones y parches:** Si un sistema no se mantiene actualizado con las últimas correcciones de seguridad, podría tener vulnerabilidades intrínsecas que los atacantes podrían explotar.

Métricas Suplementarias

El grupo de métricas suplementarias incluye métricas que proporcionan contexto, así como describen y miden atributos extrínsecos adicionales de una vulnerabilidad. Las métricas suplementarias son proporcionadas por un proveedor, son opcionales y no tienen un impacto en la puntuación numérica final del CVSS-B calculado.

El uso de cada métrica dentro del grupo de métricas suplementarias debe ser determinado por el consumidor de la puntuación, permitiendo el uso de un sistema de análisis de riesgos del usuario final para aplicar una gravedad localmente significativa a las métricas y valores. Las organizaciones pueden asignar luego la importancia y/o el impacto efectivo de cada métrica, o conjunto de métricas, otorgándoles más, menos o absolutamente ningún efecto en la decisión.

Las métricas y valores simplemente transmitirán características *extrínsecas adicionales de la propia vulnerabilidad.

* "Extrínseco" se refiere a algo que proviene o es influenciado por factores externos en lugar de ser parte de la naturaleza inherente de algo. En el contexto de las vulnerabilidades de seguridad, "extrínseco" se refiere a debilidades que no son inherentemente parte del diseño o funcionamiento del sistema, sino que resultan de factores externos o de interacciones con otros sistemas, usuarios o elementos del entorno.

Las vulnerabilidades extrínsecas se caracterizan por depender de condiciones específicas que están fuera del control directo del sistema o componente en cuestión. Estas condiciones externas pueden hacer que un sistema sea más vulnerable de lo que sería por sí solo. Algunos ejemplos de características de vulnerabilidades extrínsecas incluyen:

1. **Dependencia de factores externos:** La vulnerabilidad solo es explotable si se cumplen ciertas condiciones externas, como una configuración específica del sistema, la presencia de ciertos programas o la interacción con otros sistemas.
2. **Interacción del usuario:** La explotación de la vulnerabilidad requiere la interacción activa de un usuario o un atacante, como hacer clic en un enlace o proporcionar información sensible.
3. **Condiciones del entorno:** La vulnerabilidad solo es explotable en ciertos entornos o redes, lo que significa que no sería una amenaza en todos los contextos.
4. **Dependencia de datos externos:** La vulnerabilidad se basa en datos o entradas proporcionadas desde fuera del sistema, como datos de usuario o de red.
5. **Integración con otros sistemas:** La vulnerabilidad surge cuando un sistema interactúa con otros sistemas, lo que puede exponer debilidades que no existirían en un aislamiento completo.
6. **Cambios en la infraestructura:** Los cambios en la infraestructura, como actualizaciones de software o configuraciones, pueden exponer nuevas vulnerabilidades extrínsecas.

Métricas de Amenaza

El grupo de métricas de Amenazas refleja las características de una vulnerabilidad relacionadas con la amenaza que pueden cambiar con el tiempo, pero no necesariamente en diferentes entornos de usuario. Por ejemplo, la confirmación de que la vulnerabilidad no ha sido explotada ni cuenta con ningún código de concepto o instrucciones de prueba disponibles públicamente disminuirá la puntuación de CVSS resultante.

Métricas del Entorno

El grupo de métricas de entorno representa las características de una vulnerabilidad que son relevantes y únicas para el entorno particular de un usuario. Las consideraciones incluyen la presencia de controles de seguridad que pueden mitigar algunas o todas las consecuencias de un ataque exitoso, así como la importancia relativa de un sistema vulnerable dentro de una infraestructura tecnológica. Esta categoría suele ser completada por el consumidor.

Puntaje de CVSS versión 4.0

Se asigna una puntuación CVSS a la vulnerabilidad de un sistema en función de las métricas Base, de Amenazas y de Entorno, lo que da como resultado una Calificación de Severidad Cualitativa.

La puntuación Base es determinada por un Investigador de Seguridad u otro proveedor de puntuación para ayudar a los consumidores a responder a una vulnerabilidad. La puntuación de Amenazas y de Entorno es determinada por un Analista de Seguridad u otro oficial con el fin de tomar medidas apropiadas en respuesta a una vulnerabilidad.

El Vector de Cadena es una representación de los valores métricos resultantes de la evaluación de vulnerabilidad. El Vector de Cadena es una cadena de texto formateada específicamente que contiene cada valor asignado a cada métrica.

El nuevo sistema de CVSS versión 4.0

CVSS ya no se limita solo a una puntuación Base. Se ha añadido una nueva nomenclatura para identificar combinaciones de Base (CVSS-B), Base + Amenazas (CVSS-BT), Base + Entorno (CVSS-BE) y Base + Amenazas + Entorno (CVSS-BTE).

CVSS v.4.0 cuenta con una granularidad más detallada a través de la adición de nuevas métricas y valores Base:

Nueva métrica Base: Requisitos de Ataque (AT).

Nuevos valores de métrica Base: Interacción del Usuario (UI): Pasiva (P) y Activa (A).

CVSS v.4.0 presenta una mejora en la divulgación de las métricas de Impacto:

El alcance ha sido retirado. (Scope)

Evaluación explícita del impacto en el Sistema Vulnerable (VC, VI, VA) y en los Sistemas Subsiguientes (SC, SI, SA).

El grupo de métricas Temporales ha sido renombrado como el grupo de métricas de Amenazas:

Las métricas de Amenazas se han simplificado y aclarado. Los niveles de Remediación (RL) y la Confianza en el Informe (RC) han sido retirados. La Madurez del Exploit "Código" se ha renombrado a Madurez del Exploit (E), con valores más claros.

Se ha añadido un nuevo grupo de métricas Suplementarias para transmitir atributos extrínsecos adicionales de una vulnerabilidad que no afectan a la puntuación final CVSS-BTE:

Seguridad (S)

Automatizable (A)

Recuperación (R)

Densidad de Valor (V)

Esfuerzo de Respuesta a la Vulnerabilidad (RE)

Urgencia del Proveedor (U)

CVSS v.4.0 presenta un enfoque adicional en OT/ICS/Seguridad:

Seguridad Evaluada por el Consumidor (MSI:S, MSA:S).

Seguridad Evaluada por el Proveedor a través de la métrica Suplementaria de Seguridad (S).

Métricas Base y Suplementarias - Guía (CVSS-B)

Vector de ataque

Esta métrica refleja el contexto en el cual es posible la explotación de una vulnerabilidad. El Vector de Ataque representa el método más amplio de ataque al sistema vulnerable. Cuanto más amplias sean las fuentes de ataque posibles, mayor será la gravedad y, en última instancia, la puntuación CVSS.

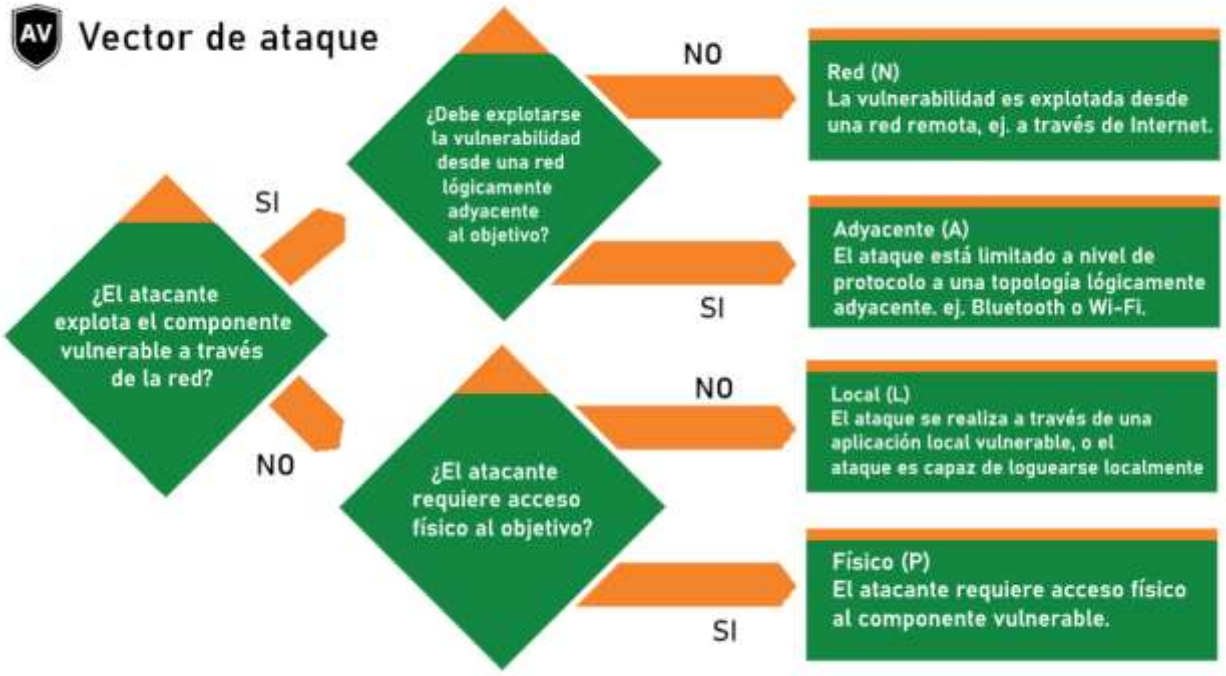
Vectores de ataque

Adyacente: Posibilidad de que un atacante pueda utilizar la explotación exitosa de una vulnerabilidad en un componente para comprometer otro componente que esté conectado o cercano al primero. Esto puede ocurrir cuando un componente vulnerable comparte recursos o interacciones con otros componentes. **. Físico:** Un atacante podría explotar una vulnerabilidad en un sistema o componente al acceder físicamente al dispositivo, equipo o infraestructura en cuestión.

Local: Un vector de ataque local implica que el atacante ya está dentro del entorno del sistema y puede interactuar con él, ya sea físicamente o a través de una sesión de usuario. Esto podría ser, por ejemplo, un usuario malintencionado que tiene acceso a una computadora en la que está buscando explotar una vulnerabilidad en un programa o sistema operativo.

Red: Un atacante podría explotar una vulnerabilidad en un sistema, aplicación o dispositivo a través de una red, sin necesidad de tener acceso físico o local al sistema objetivo. En otras palabras, es un método de ataque que se lleva a cabo de forma remota, utilizando las capacidades de comunicación de una red.

Identificar el vector de ataque



Complejidad del ataque y sus requerimientos

Complejidad del ataque

La Complejidad del Ataque describe las condiciones que están más allá del control del atacante y que deben existir para explotar la vulnerabilidad.

La Complejidad del Ataque captura las acciones medibles que el atacante debe llevar a cabo para evadir o eludir activamente las características de seguridad integradas existentes, como *ASLR o *DEP.

Esta métrica tiene la intención de capturar los mecanismos de seguridad utilizados por el sistema vulnerable y no está relacionada con la cantidad de tiempo o intentos que tomarían para que el atacante tenga éxito.

*** ASLR:** Característica de seguridad integrada en sistemas operativos modernos para proteger contra ataques de desbordamiento de búfer y otras vulnerabilidades de explotación. Su objetivo principal es dificultar la previsibilidad de las direcciones de memoria en un proceso, lo que hace que sea más difícil para un atacante aprovechar una vulnerabilidad en un programa.

*** DEP:** Característica de seguridad integrada en sistemas operativos modernos y hardware de procesadores que ayuda a prevenir la ejecución de código malicioso en áreas de memoria

designadas como no ejecutables. Su objetivo principal es proteger contra ataques que intentan explotar vulnerabilidades de desbordamiento de búfer y ejecutar código malicioso en áreas de memoria que normalmente solo deberían contener datos.

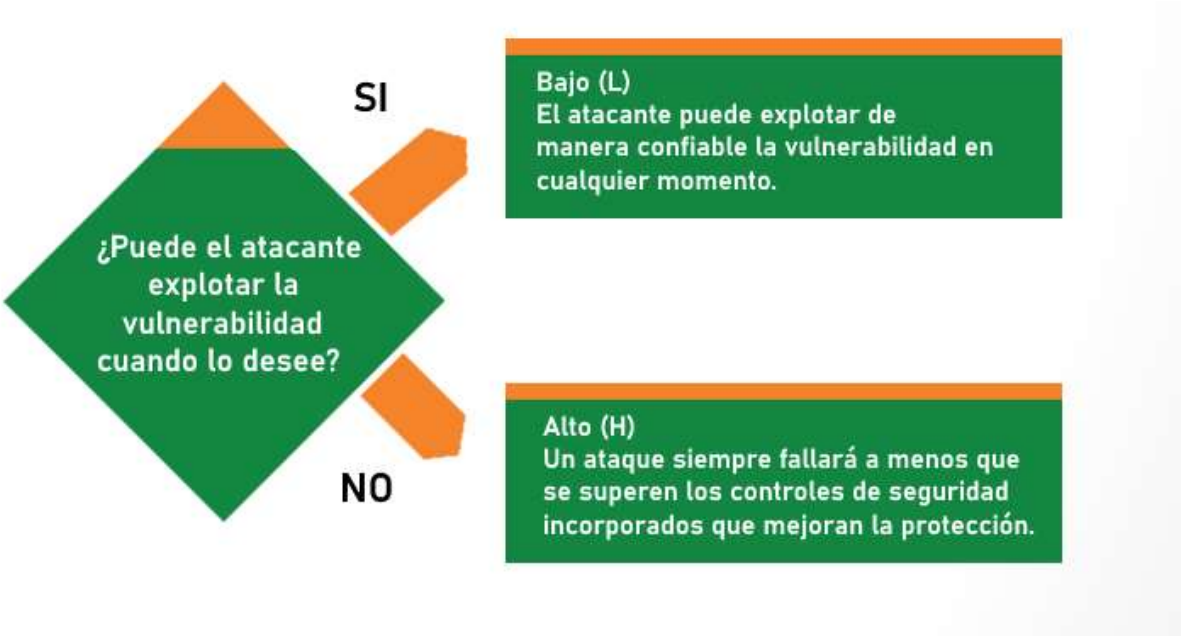
Requerimientos del ataque

Los Requisitos de Ataque capturan las condiciones previas de implementación y ejecución del sistema vulnerable que habilitan el ataque.

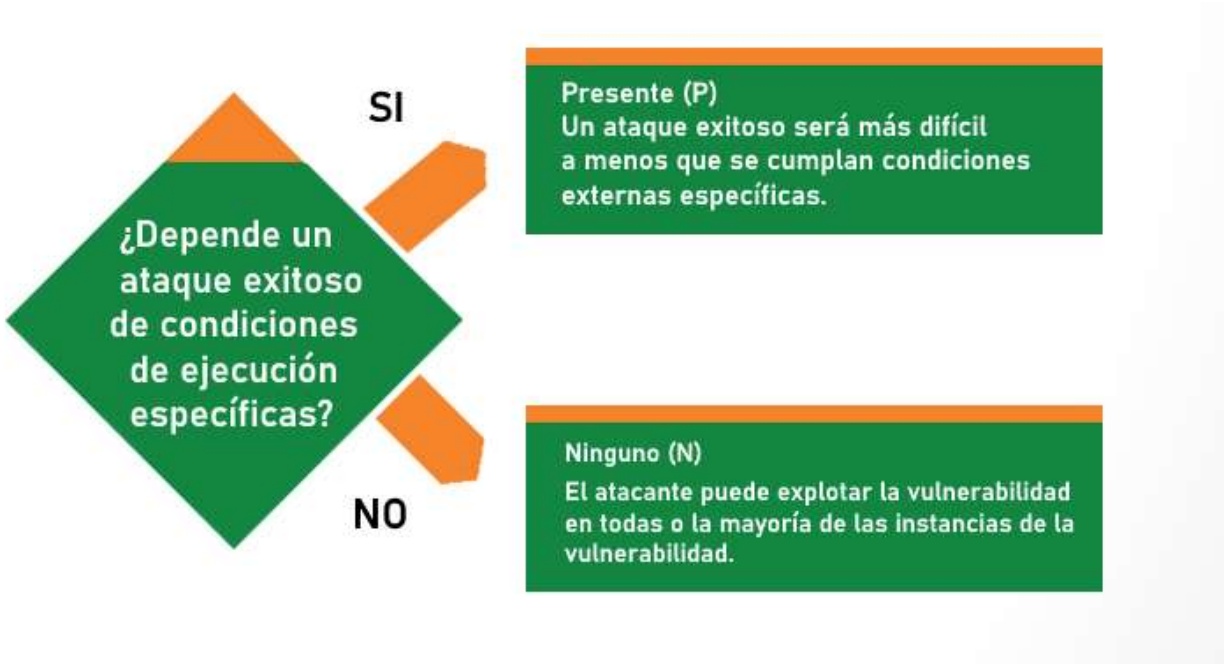
Estos difieren de las técnicas/tecnologías de mejora de seguridad (Complejidad del Ataque), ya que el propósito principal de estas condiciones no es mitigar los ataques de manera explícita, sino que surgen naturalmente debido a la implementación y ejecución del componente vulnerable.

El éxito del ataque depende de la presencia de condiciones específicas de implementación y ejecución del software vulnerable que habilita el ataque.

Determinar la complejidad del ataque



Determinar los requerimientos del ataque

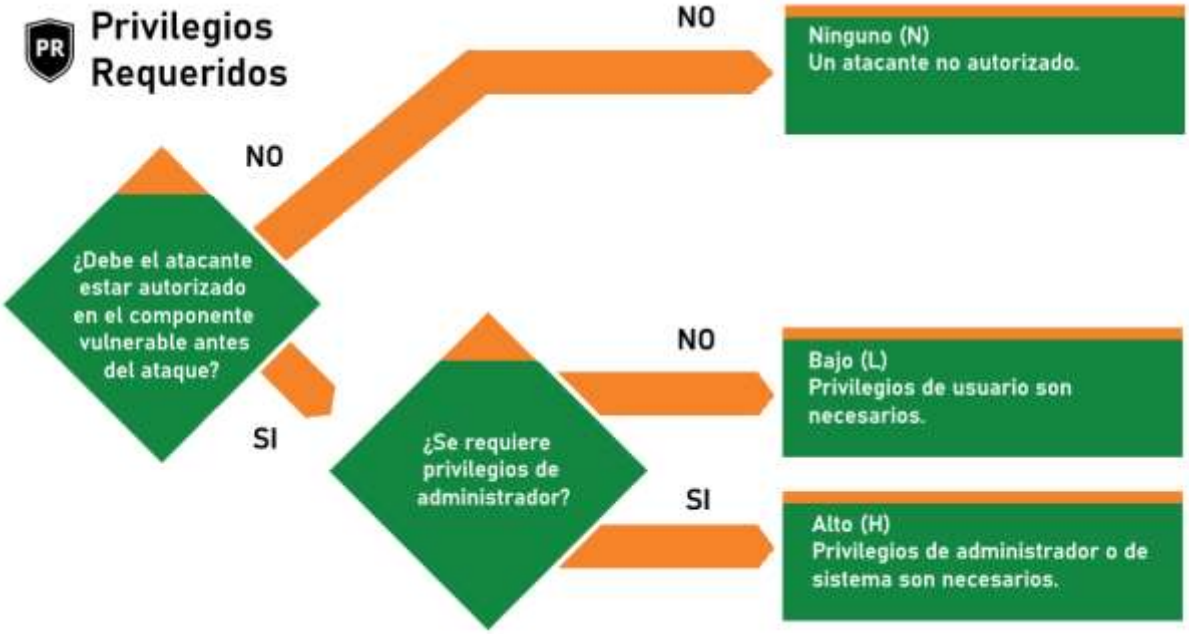


Privilegios necesarios

Esta métrica describe el nivel de privilegios que un atacante debe tener antes de lograr explotar la vulnerabilidad.

La pregunta principal a responder al considerar los privilegios necesarios es: ¿La explotación exitosa de esta vulnerabilidad requiere que el atacante posea credenciales de autenticación específicas?

Determinar los privilegios necesarios

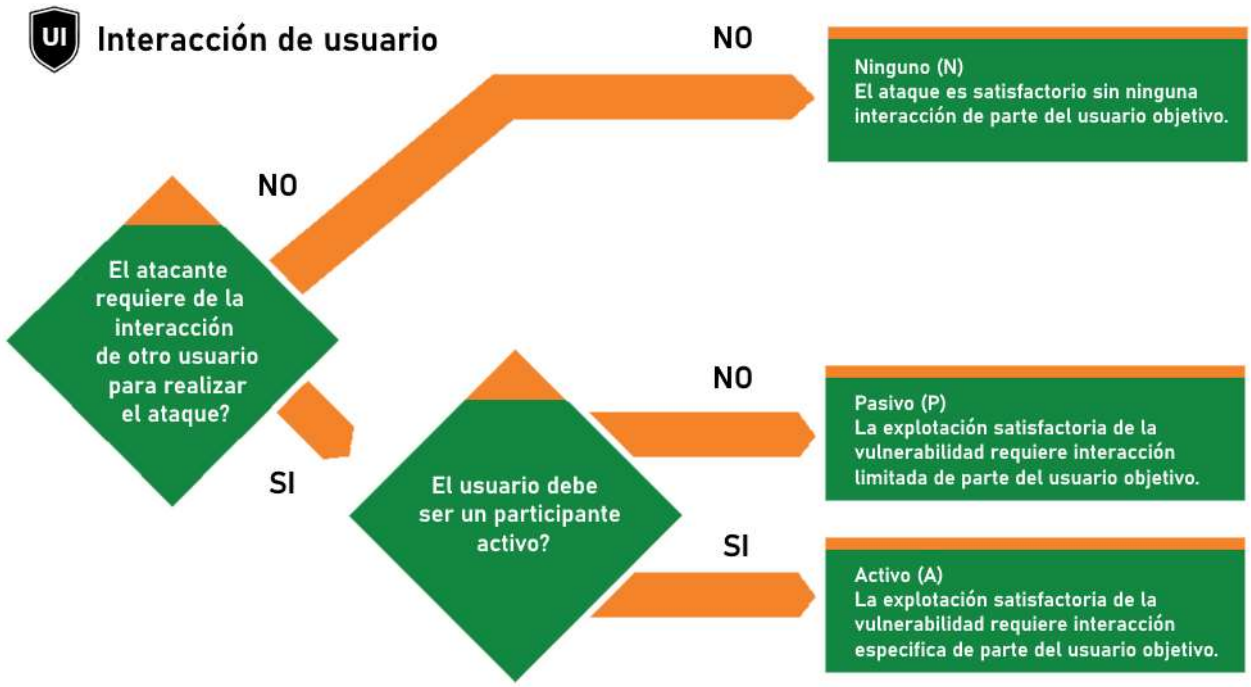


Interacción de usuario

Denota la necesidad de que un usuario humano, distinto al atacante, participe en la misión exitosa del componente vulnerable.

Esta métrica determina si la vulnerabilidad puede ser explotada únicamente a voluntad del atacante, o si un participante no deseado por separado debe participar de alguna manera.

Determinar la interacción del usuario



Métrica de impacto

Al identificar valores para las métricas de impacto, los proveedores de puntuación deben tener en cuenta los impactos tanto en el Sistema Vulnerable como fuera de él. Estos impactos se establecen mediante dos conjuntos de métricas de impacto: el impacto en el Sistema Vulnerable y el impacto en Sistemas Subsiguientes.

Confidencialidad La Confidencialidad mide el impacto en la confidencialidad de los recursos de información gestionados por un sistema de software debido a una vulnerabilidad explotada exitosamente.

La confidencialidad se refiere a limitar el acceso y la divulgación de información solo a usuarios autorizados, así como prevenir el acceso o la divulgación a usuarios no autorizados. La puntuación resultante es mayor cuando la pérdida para el sistema afectado es más alta.

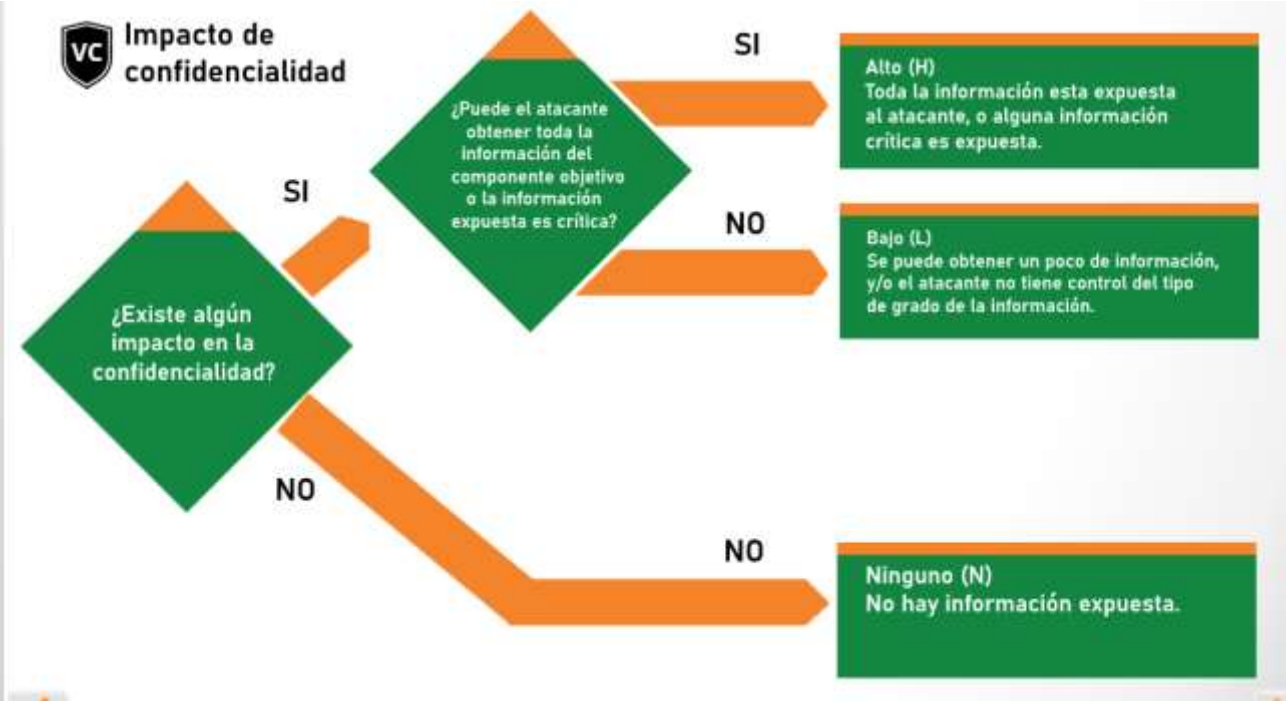
Integridad La Integridad mide el impacto en la integridad de una vulnerabilidad explotada exitosamente. La integridad se refiere a la confiabilidad y veracidad de la información. La puntuación resultante es mayor cuando la consecuencia para el sistema afectado es más alta.

Disponibilidad La Disponibilidad mide el impacto en la disponibilidad del sistema afectado como resultado de una vulnerabilidad explotada exitosamente.

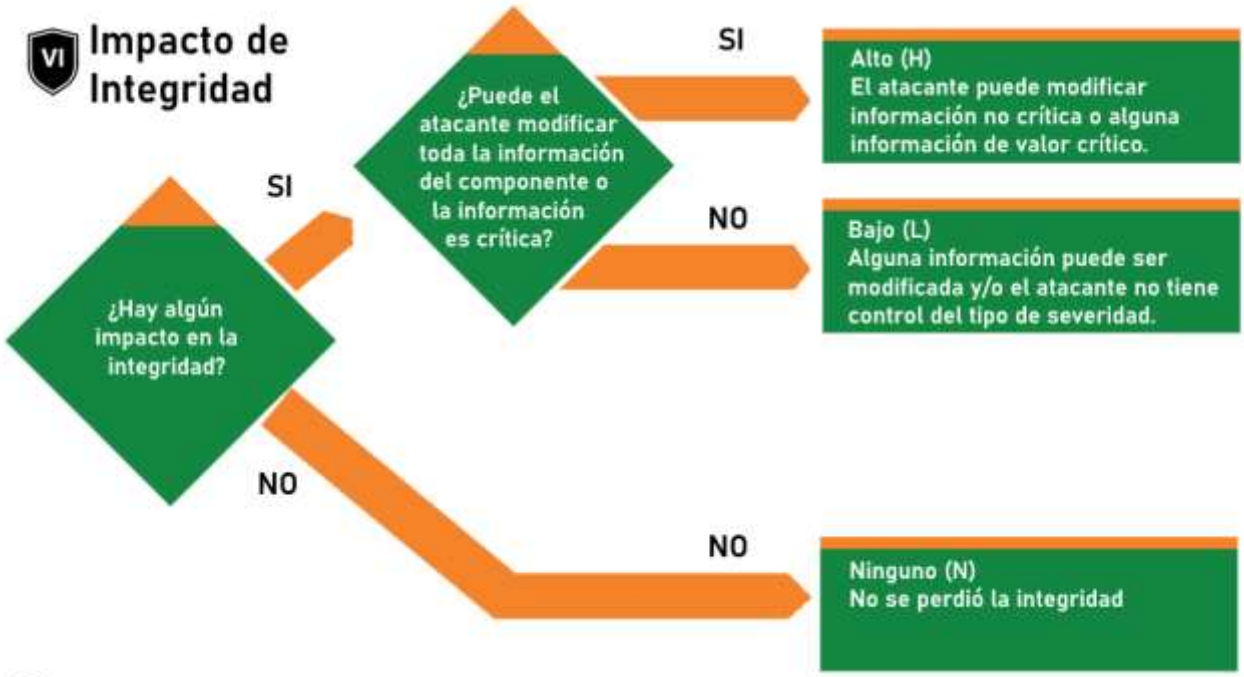
Mientras que las métricas de impacto en la Confidencialidad e Integridad se refieren a la pérdida de confidencialidad o integridad de los datos (por ejemplo, información, archivos) utilizados por el sistema afectado, esta métrica se refiere a la pérdida de disponibilidad del propio sistema afectado, como un servicio en red (por ejemplo, web, base de datos, correo electrónico).

Dado que la disponibilidad se refiere a la accesibilidad de los recursos de información, los ataques que consumen ancho de banda de red, ciclos de procesador o espacio en disco afectan la disponibilidad de un sistema subsiguiente. La puntuación resultante es mayor cuando la consecuencia para el sistema afectado es más alta.

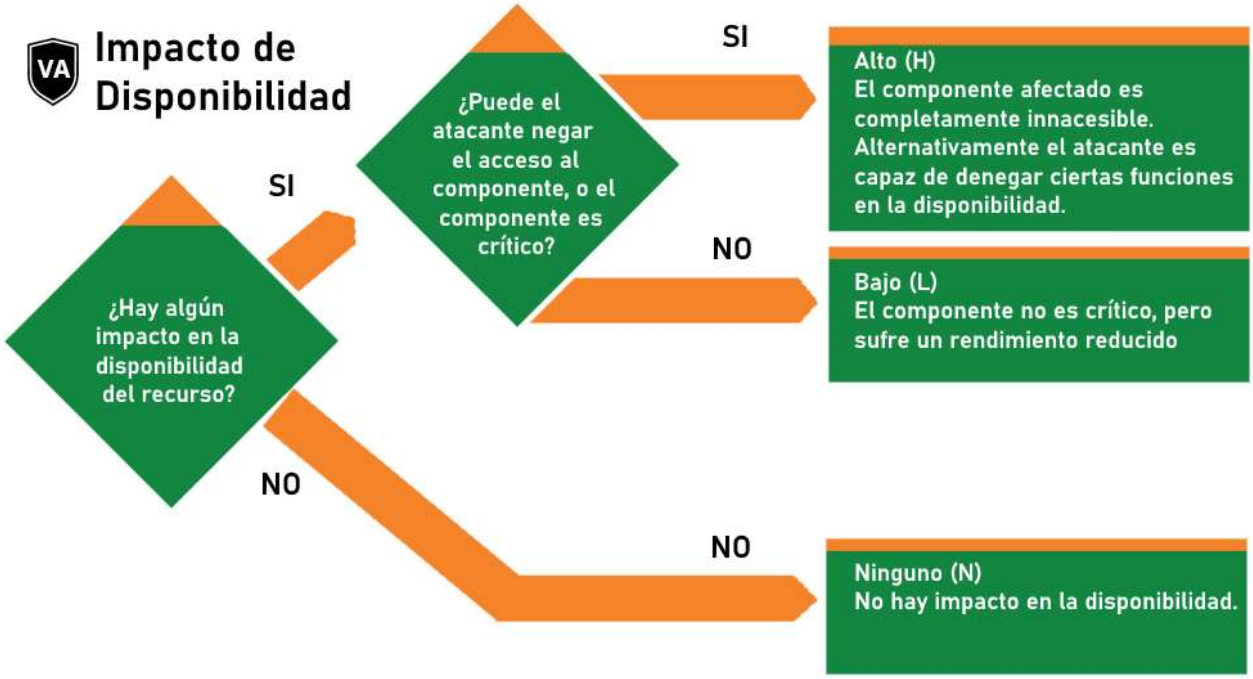
Determinar el nivel de impacto sobre la confidencialidad



Determinar el nivel de impacto sobre la integridad



Determinar el nivel de impacto sobre la disponibilidad



Es importante destacar que las métricas de explotabilidad no importarán si no hay impacto. Esto significa que si todas las métricas de impacto se establecen en "Ninguno", la puntuación se mantendrá en 0 para todas las combinaciones de métricas Base, Suplementarias, de Amenazas y de Entorno.

Métricas suplementarias

Las métricas suplementarias son un nuevo grupo de métricas opcional proporcionado por el Proveedor que describe y mide atributos extrínsecos adicionales de una vulnerabilidad.

Esta información contextual puede utilizarse de manera diferente en cada entorno informático a discreción del consumidor. Ninguna métrica tendrá ningún impacto en la puntuación CVSS final calculada.

Las organizaciones/consumidores pueden asignar importancia o acciones específicas en función de estos valores métricos según consideren apropiado, otorgándoles más, menos o absolutamente ningún efecto en la priorización.

Las métricas y valores simplemente transmitirán características extrínsecas adicionales de la propia vulnerabilidad.

Seguridad

Cuando un sistema tiene un uso previsto o una aptitud de propósito alineada con la seguridad, es posible que explotar una vulnerabilidad dentro de ese sistema tenga un impacto en la seguridad que puede ser representado en el grupo de Métricas Suplementarias.

La seguridad utiliza los siguientes valores:

No Definido (X): No tiene ninguna relación directa con sistemas de seguridad física o control de acceso. En este caso, la métrica de "Seguridad" podría estar definida como "No definido", ya que no hay ningún impacto en la seguridad física o en sistemas de seguridad.

Negligible (N): Tiene relación directa con sistemas de seguridad física o control de acceso pero no todos fueron vulnerados de manera exitosa, podría definirse como "Negligible". **Presente (P):** Tiene relación directa con sistema de seguridad física o control de acceso y aún así fue vulnerado, esto cuando hablamos de un único activo de ataque que su único objeto vulnerable que era seguro fue vulnerado exitosamente aún así teniendo medidas de seguridad.

Automatización

La métrica Automatizable captura la respuesta a la pregunta: "¿Puede un atacante automatizar eventos de explotación para esta vulnerabilidad en múltiples objetivos?"

La métrica Automatizable se basa en los pasos 1-4 de la cadena de ataque. Estos pasos son:

Reconocimiento, preparación de armamento, entrega y explotación.

Utiliza los siguientes valores:

No Definido (X): No se tiene información suficiente para determinar si la explotación puede automatizarse o no. En este caso, la métrica de "Automatización" podría estar definida como "No definido".

No (N): La explotación no puede automatizarse. En este caso, la métrica de "Automatización" podría estar definida como "No".

Sí (Y): La explotación puede automatizarse. En este caso, la métrica de "Automatización" podría estar definida como "Sí".

Recuperación

La Recuperación describe la capacidad de un componente o sistema para recuperar servicios (en términos de rendimiento y disponibilidad) después de que se haya realizado un ataque.

Recuperación utiliza los siguientes valores:

No Definido (X): No se tiene suficiente información para determinar cómo afectaría la recuperación del sistema. En este caso, la métrica de "Recuperación" podría estar definida como "No definido".

Automático (A): El servidor está configurado con mecanismos automáticos de detección y recuperación que pueden reiniciar automáticamente el servicio en caso de un fallo. En este caso, la métrica de "Recuperación" podría estar definida como "Automático". Usuario (U): La recuperación requeriría la intervención manual de un administrador para eliminar el código malicioso y restaurar el sistema. La métrica de "Recuperación" podría estar definida como "Usuario".

Irrecuperable (I): Una vez que se explota la vulnerabilidad, los datos afectados no pueden ser recuperados, lo que resulta en una pérdida permanente. En este caso, la métrica de "Recuperación" podría estar definida como "Irrecuperable".

Urgencia del proveedor

Para facilitar un método estandarizado para incorporar una evaluación adicional proporcionada por el proveedor, CVSS ha propuesto adoptar una Métrica Suplementaria opcional llamada Urgencia del Proveedor.

La Urgencia del Proveedor utiliza Niveles de Urgencia:

Rojo: Urgencia más alta

Ámbar: Urgencia moderada

Verde: Urgencia reducida

Claro: Baja o nula urgencia

Densidad del valor

Describe los recursos sobre los cuales el atacante obtendrá control con un solo evento de explotación.

Utiliza los siguientes valores:

No Definido (X): No se tiene información suficiente para determinar cómo se distribuyen los valores posibles para la métrica de impacto base. En este caso, la métrica de "Densidad del valor" podría estar definida como "No definido".

Difuso (D): La explotación de la vulnerabilidad puede tener un impacto variable en diferentes partes del sistema, afectando a varios componentes de manera dispersa. En este caso, la métrica de "Densidad del valor" podría estar definida como "Difuso".

Concentrado (C): La explotación tiene lugar en una única área funcional, y su impacto es significativo y concentrado, la métrica de "Densidad del valor" podría estar definida como "Concentrado".

Esfuerzo de respuesta de la vulnerabilidad

La intención del Esfuerzo de Respuesta a la Vulnerabilidad es proporcionar información adicional sobre cuán difícil es para los consumidores brindar una respuesta inicial al impacto de las vulnerabilidades en los productos y servicios desplegados en su infraestructura.

El consumidor puede luego tener en cuenta esta información adicional sobre el esfuerzo requerido al aplicar mitigaciones y/o programar remedios. El Esfuerzo de Respuesta a la Vulnerabilidad utiliza los siguientes valores:

No Definido (X): Aún no se tiene suficiente información para determinar el nivel de esfuerzo necesario para abordarla. En este caso, la métrica de "Esfuerzo de Respuesta a la Vulnerabilidad" podría estar definida como "No definido".

Bajo (L): La corrección para esta vulnerabilidad podría ser relativamente simple, como aplicar un parche de software o actualizar una configuración. En este caso, la métrica de "Esfuerzo de Respuesta a la Vulnerabilidad" podría estar definida como "Bajo".

Moderado (M): Se podrían necesitar cambios en la configuración, actualizaciones de software y cierta coordinación interna para mitigar el impacto. La métrica de "Esfuerzo de Respuesta a la Vulnerabilidad" podría estar definida como "Moderado".

Alto (H): La explotación de esta vulnerabilidad podría requerir una respuesta compleja, que incluye cambios en múltiples componentes, pruebas exhaustivas y una planificación detallada para asegurarse de que la mitigación no cause interrupciones no deseadas. En este caso, la métrica de "Esfuerzo de Respuesta a la Vulnerabilidad" podría estar definida como "Alto".

Resumen

Métricas de Amenaza y Entorno - Guía (CVSSBTE Completo)

Resumen comparativo de las métricas:

El grupo de métricas Base representa las características intrínsecas de una vulnerabilidad que son constantes en el tiempo y en diferentes entornos. El grupo de métricas de Amenazas refleja las características de una vulnerabilidad que pueden cambiar con el tiempo, pero no en diferentes entornos de usuario. **.** El grupo de métricas Ambientales representa las características de una vulnerabilidad que son relevantes y únicas para el entorno particular de un usuario.

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.

Las métricas de amenazas se derivan de la Inteligencia de Amenazas recopilada por el consumidor de Gestión de Vulnerabilidades.

Madurez del Exploit

La métrica de amenaza más vital es la Madurez del Exploit.

La Madurez del Exploit mide la probabilidad de que un actor malintencionado intente un ataque contra una vulnerabilidad del sistema. La Madurez del Exploit se basa típicamente en el estado actual de las técnicas de explotación, la disponibilidad de código de explotación o la explotación activa y en el sitio. Utiliza los siguientes valores:

No definido (X): Asignar un valor de No Definido (X) indica que el atributo de Madurez del Exploit no está siendo utilizado. Esto se debe a que no se dispone de una inteligencia de amenazas confiable para determinar las características de Madurez del Exploit.

Un valor de No Definido significa que los cálculos de vulnerabilidad asumen el peor escenario posible para todas las vulnerabilidades. Asignar este valor no influirá en la puntuación resultante.

Atacado (A): Un valor de Atacado (A) indica que las fuentes de inteligencia de amenazas han determinado que debe aplicarse una de las siguientes situaciones:

Se han informado ataques dirigidos a esta vulnerabilidad (intentados o exitosos).

Se han hecho públicas o privadas soluciones para simplificar los intentos de explotación de la vulnerabilidad (como kits de herramientas de explotación).

Prueba de concepto (P): Un valor de Prueba de Concepto (P), también conocido como POC, indica que las fuentes de inteligencia de amenazas han determinado que se debe cumplir cada uno de los siguientes puntos: Código o técnicas de prueba de concepto están disponibles públicamente.

No se tiene conocimiento de intentos reportados para explotar la vulnerabilidad.

No se tiene conocimiento de soluciones disponibles públicamente utilizadas para simplificar los intentos de explotación de la vulnerabilidad (es decir, el valor Atacado (A) no se aplica).

No reportado (U): Un valor de No Reportado (U) indica que las fuentes de inteligencia de amenazas han determinado que se deben cumplir los siguientes puntos: No se tiene conocimiento de una prueba de concepto disponible públicamente.

No se tiene conocimiento de intentos reportados para explotar la vulnerabilidad.

No se tiene conocimiento de soluciones disponibles públicamente utilizadas para simplificar los intentos de explotación de la vulnerabilidad (es decir, ni el valor Prueba de Concepto (P) ni el valor Atacado (A) se aplican).

Determinar la madurez del Exploit

Métricas base y de seguridad modificadas - Afecta

Las métricas Base modificadas y la Seguridad son Métricas Ambientales que permiten al consumidor personalizar o ajustar de manera efectiva los valores de la puntuación Base del CVSS según los controles de seguridad y/o arquitectura específicos del entorno del sistema vulnerable.

Valores para las métricas base modificadas Las métricas Base modificadas brindan al consumidor la oportunidad de realizar ajustes a las métricas base según la implementación de esos sistemas en sus entornos individuales. Esto incluye controles compensatorios como:

Firewalls

Segmentación de redes

Funciones o políticas de seguridad adicionales.

También se incluyen otras situaciones, como:

Seguridad y Sistemas de Control Industrial (ICS)

Ajustes potenciales en el impacto aguas abajo relacionados con Tecnología

Operativa (OT)

Estas métricas permiten una personalización más precisa de la puntuación CVSS para reflejar el entorno y las condiciones específicas del sistema vulnerable.

Valores para las métricas de seguridad modificadas

Cuando un sistema puede tener implicaciones de seguridad según cómo o dónde se implemente, es posible que explotar una vulnerabilidad dentro de ese sistema pueda tener impactos en la seguridad, que se pueden representar aquí, en el grupo de Métricas de Entorno.

El valor de la métrica Seguridad mide el impacto en relación con la seguridad de un actor humano o participante que podría predeciblemente resultar herido como resultado de la explotación de la vulnerabilidad. A diferencia de otros valores de métricas de impacto, la Seguridad solo puede estar asociada con el conjunto de impacto en Subsecuentes Sistemas(s) y debe considerarse además de los valores de impacto N/L/H para las métricas de Disponibilidad e Integridad.

La Seguridad se considera aplicable cuando es predecible que una vulnerabilidad explotada pueda resultar en lesiones graves o peores.

Los valores de Integridad del Subsecuente Sistema Modificado (MSI) y Disponibilidad del Subsecuente Sistema Modificado (MSA) pueden establecerse en "S" cuando un ataque de explotación previsiblemente resultaría en lesiones graves o peores.

Requisitos de seguridad

El grupo de métricas Requisitos de Seguridad identifica tres métricas para medir la criticidad del sistema vulnerable. Estas métricas permiten al analista personalizar la puntuación CVSS según la importancia del activo de TI afectado para la organización del usuario, medida en términos de Confidencialidad, Integridad y Disponibilidad. Si un activo de TI respalda una función empresarial para la cual la Disponibilidad es más importante, el analista puede asignar un valor mayor a las métricas de Disponibilidad. Cada Requisito de Seguridad tiene tres valores posibles:

Bajo

Medio

Alto

Valores para los requisitos de seguridad

Requisitos de confidencialidad: El Requisito de Confidencialidad (CR) de un sistema debe basarse en el nivel de clasificación de los datos que son almacenados o utilizados por el usuario y/o aplicaciones que se ejecutan en el sistema objetivo. La encriptación de los datos en reposo en este dispositivo también debe ser considerada al establecer el Requisito de Confidencialidad. Los datos que atraviesan un dispositivo sin ser consumidos ni procesados (por ejemplo, un switch o un firewall) no deben tenerse en cuenta al evaluar este atributo.

Requisitos de integridad: Los Requisitos de Integridad (IR) de un sistema se centran en la importancia de la precisión de los datos que almacena o utiliza. Los datos que atraviesan un dispositivo sin ser consumidos ni procesados (por ejemplo, un switch o un firewall) no deben tenerse en cuenta al evaluar este atributo. El uso de encriptación en los datos en reposo no debe ser considerado para este atributo.

Requisitos de disponibilidad: El Requisito de Disponibilidad (AR) de un sistema debe basarse en los requisitos de tiempo de actividad y redundancia del dispositivo o las aplicaciones alojadas por el dispositivo. Los dispositivos que forman parte de clústeres redundantes tendrán requisitos de Disponibilidad más bajos.

Determinar el valor para los requisitos de seguridad (Confidencialidad)

Determinar el valor para los requisitos de seguridad (Integridad)

Determinar el valor para los requisitos de seguridad (Disponibilidad)

Resumen

Cadena de vector

La Cadena de Vectores CVSS v.4.0 es una representación de texto de un conjunto de métricas CVSS: La Cadena de Vectores comienza con la etiqueta "CVSS:" y una representación numérica de la versión actual, "4.0." Cada métrica está precedida por una barra diagonal, "/", que actúa como delimitador. Cada métrica consiste en el nombre de la métrica en forma abreviada, seguido de dos puntos, ":", y su valor de métrica asociado en forma abreviada.

Escala de Calificación de Severidad Cualitativa

Todos los puntajes pueden ser asignados a las calificaciones cualitativas definidas aquí:

Escala	Puntuación de CVSS
Ninguno	0.0
Bajo	0.1 - 3.9
Medio	4.0 - 6.9
Alto	7.0 - 8.9
Crítico	9.0 - 10.0

Herramientas para seguir profundizando

Curso de CVSS v4.0: https://learn.first.org/catalog/info/id:126,cms_featured_course:1
Calculadora de puntuación CVSS v4.0: https://www.first.org/cvss/calculator/4.0