Engineer

CVE

catálogo público con un ID por vulnerabilidad divulgada

Qué es

CVE, abreviatura de Common Vulnerabilities and Exposures, es el catálogo público de vulnerabilidades de ciberseguridad divulgadas públicamente, con un CVE Record o registro CVE para cada una. El programa CVE describe su misión como identificar, definir y catalogar esas vulnerabilidades para que dos personas o herramientas puedan referirse a un fallo sabiendo que hablan del mismo. La palabra se utiliza para el programa, para la lista y, de forma menos estricta, para una entrada individual, como en «esa biblioteca tiene dos CVE pendientes».

Cada registro lleva un identificador CVE. El formato es el prefijo `CVE`, un año de cuatro cifras y un número de secuencia de cuatro cifras o más, de modo que `CVE-1999-0067`, `CVE-2019-12345` y `CVE-2021-7654321` son válidos; el programa no fija ningún límite superior a la longitud del número de secuencia. El año es aquel en que se reservó el ID o se hizo pública la vulnerabilidad. En palabras del propio programa, «la parte del año no se utiliza para indicar cuándo se descubrió la vulnerabilidad».

Los ID no los reparte una única oficina central. Las CVE Numbering Authorities, o CNA, son proveedores, investigadores, proyectos de código abierto, equipos de respuesta a emergencias, operadores de servicios en línea, proveedores de programas de recompensas por errores y consorcios autorizados por el programa para asignar ID y publicar registros, cada uno dentro de su ámbito. Todos los registros CVE los añade una CNA, no hay que pagar ni firmar un contrato para convertirse en una y, desde 2016, el programa trabaja activamente para incorporar más.

Un registro pasa por tres estados. Empieza como Reserved (reservado), cuando una CNA ha obtenido un ID que las partes implicadas utilizan para coordinar el trabajo inicial sobre la vulnerabilidad antes de su divulgación. Pasa a Published

(publicado) cuando la CNA ha completado al menos el ID, una descripción breve, los productos y versiones afectados y una referencia pública. Si el ID ya no debe utilizarse, pasa a Rejected (rechazado), y el registro permanece en la lista para que cualquiera que conserve el ID pueda ver que ya no es válido.

La idea se remonta a 1999. Dos ingenieros de MITRE, David E. Mann y Steven M. Christey, presentaron el concepto en un documento técnico durante un taller de la Universidad Purdue en enero de 1999, y la lista se hizo pública en septiembre de 1999 con 321 registros.

Utilice el concepto en una decisión

Aplique «¿Qué es CVE?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

1.000 reglas RBAC para servidores Linux Póngase en contacto →

Por qué importa

Un informe sobre una vulnerabilidad solo es útil si quienes lo leen pueden saber si trata del mismo problema que otro informe. Un identificador CVE lo resuelve: dos avisos, un hallazgo de un escáner y un ticket con el mismo ID se refieren al mismo fallo. Numerosos grandes proveedores de sistemas operativos incluyen identificadores CVE en sus avisos para que todos dispongan del identificador desde que se anuncia un problema, y productos y servicios de seguridad de todo el mundo incorporan registros CVE en sus informes.

Otros servicios se construyen sobre la lista, no a su lado. La National Vulnerability Database de Estados Unidos, puesta en marcha por NIST en 2005, es un programa independiente que parte de los registros CVE y añade su propio análisis a cada uno. El catálogo Known Exploited Vulnerabilities (KEV) de CISA enumera fallos que se ha observado que los atacantes utilizan. Cada entrada indica su identificador CVE y enlaza al registro correspondiente.

Lo más útil que conviene saber sobre CVE es lo que no es. La gravedad se mide por separado con CVSS, Common Vulnerability Scoring System, un estándar gestionado por FIRST, una organización sin ánimo de lucro con sede en Estados Unidos cuya misión es ayudar a los equipos de respuesta a incidentes de

seguridad informática de todo el mundo. CVSS versión 4.0 puntúa una vulnerabilidad de 0 a 10 mediante los grupos de métricas Base, Threat, Environmental y Supplemental (base, amenaza, entorno y complementarias), y traduce el número a None, Low, Medium, High y Critical (ninguna, baja, media, alta y crítica), con Critical entre 9,0 y 10,0. CVE Record Format permite a una CNA incluir una puntuación CVSS en su registro, pero la puntuación pertenece a CVSS, no al ID: un fallo puede tener puntuaciones distintas de distintos editores o no tener ninguna.

Tampoco es una clase de debilidad. Common Weakness Enumeration, CWE, es una lista de debilidades desarrollada por la comunidad: condiciones del software, firmware, hardware o un servicio que, en las circunstancias adecuadas, pueden dar lugar a una vulnerabilidad. El programa CVE describe las CWE como las causas raíz de los registros CVE. Una CVE identifica un fallo en un producto; una CWE identifica el tipo de error que hay detrás. La inyección SQL, por ejemplo, es la debilidad CWE-89, y cada producto en el que se descubre ese error recibe su propio identificador CVE.

Cómo se aplica en la práctica

Shellshock, el fallo de Bash de 2014, muestra los tres sistemas juntos. cve.org presenta sus registros en CVE Record Format, un formato JSON, y la parte superior de este dice lo siguiente (con campos recortados y reordenados):


```
{
  "dataType": "CVE_RECORD",
  "dataVersion": "5.1",
  "cveMetadata": {
    "cveId": "CVE-2014-6271",
    "assignerShortName": "debian",
    "state": "PUBLISHED",
    "dateReserved": "2014-09-09T00:00:00.000Z",
    "datePublished": "2014-09-24T18:00:00.000Z",
    "dateUpdated": "2025-10-22T00:05:36.342Z"
  }
}
```


Debian, actuando como CNA, reservó el ID el 9 de septiembre de 2014 y publicó el registro quince días después. Su descripción dice que Bash hasta la versión 4.3 procesa el texto que sigue a una definición de función en el valor de una variable de entorno, lo que permite a un atacante remoto ejecutar código arbitrario mediante un entorno preparado. También registra que la primera corrección

era incorrecta y que la parte que seguía abierta recibió un ID propio, CVE-2014-7169. Los equipos que aplicaron un parche una vez y se detuvieron siguieron expuestos.

El registro contiene después contenedores de tres fuentes distintas. El contenedor CNA incluye la descripción y las referencias de Debian. CVE Program Container añade referencias propias. Un tercero, de un Authorized Data Publisher y titulado CISA ADP Vulnrichment, añade lo que el identificador CVE por sí solo no contiene:

```
{
  "cvssV3_1": {
    "version": "3.1",
    "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H",
    "baseScore": 9.8,
    "baseSeverity": "CRITICAL"
  }
}
```

La cadena del vector expone el razonamiento que hay detrás de 9,8: un ataque por la red, de baja complejidad, que no necesita privilegios ni interacción del usuario y tiene un impacto alto en la confidencialidad, integridad y disponibilidad. El mismo contenedor vincula el fallo con CWE-78, la clase de debilidad de inyección de comandos del sistema operativo, y registra que CISA lo añadió al catálogo KEV el 28 de enero de 2022. Un solo registro contiene por tanto un ID del programa CVE, una puntuación de una versión de CVSS publicada por FIRST y una clase de debilidad de CWE, cada uno de una fuente distinta y respondiendo a una pregunta diferente.

En el día a día, los identificadores CVE importan menos como lectura que como claves. La página de seguridad describe la rutina: se enumeran los componentes con los que se construye cada sistema y se compara la lista con los avisos publicados, en lugar de confiar en ellos porque antes funcionaban. El identificador CVE permite seguir un hallazgo de esa comprobación hacia atrás hasta el aviso y hacia delante hasta la actualización que lo resuelve.

Dónde surgen los problemas

Leer la puntuación como si fuera el riesgo. Cuando nadie proporciona valores Threat o Environmental, la especificación CVSS 4.0 los completa con valores predeterminados que suponen el peor caso y señala que NVD y quienes mantienen los productos suelen publicar solo la puntuación Base. Un 9,8 en un componente inaccesible desde el exterior no es un 9,8 para usted. Etiquete las puntuaciones como pide la especificación: CVSS-B si solo se usa Base y CVSS-BTE si se aplicaron valores Threat y Environmental, y añada los valores Environmental de sus propios sistemas antes de priorizar el trabajo.

Confundir CVE, CVSS y CWE. «Una CVE de 9,8» mezcla un identificador con una puntuación, y «la CVE de inyección SQL» mezcla un fallo con una clase de fallos. Mantenga separados los tres en tickets e informes: el ID de CVE, la puntuación con su versión de CVSS y la causa raíz de CWE.

Citar un número sin su vector. FIRST exige a cualquiera que publique datos CVSS que publique el vector junto al número para que puedan examinarse las decisiones subyacentes. Un número aislado no puede verificarse, compararse entre versiones de CVSS ni ajustarse a su entorno. Guarde el vector completo, incluido el prefijo `CVSS:3.1/` o `CVSS:4.0/` que identifica la versión.

Interpretar el año como fecha de descubrimiento. El año del ID es aquel en que se reservó o el fallo se hizo público. Un ID de 2014 puede describir código publicado en la década de 1990, y un fallo encontrado en diciembre puede llevar el número del año siguiente. Utilice para las fechas los campos `dateReserved` y `datePublished` del registro, nunca el ID.

Suponer cuatro cifras. El número de secuencia tiene cuatro cifras o más sin límite superior, así que un patrón como `CVE-\d{4}-\d{4}` recorta silenciosamente los ID más largos. Utilice `^CVE-[0-9]{4}-[0-9]{4,}$` y trate el ID como una cadena, no como un número, para conservar los ceros iniciales.

Tratar un registro Rejected como si faltara. Un ID Rejected permanece en la lista a propósito, para indicar que ya no es válido. Una herramienta que lo ignore o lo cuente como un hallazgo pendiente induce a error en cualquiera de los dos sentidos. Lea el campo `state` y gestione `REJECTED` explícitamente.

Tratar el registro como terminado. El registro de Shellshock cambió por última vez en octubre de 2025, once años después de publicarse, y su entrada en KEV llegó en enero de 2022. La especificación CVSS utiliza el grupo Threat para tener en cuenta los cambios de las circunstancias de una vulnerabilidad con el tiempo. Vuelva a leer de forma programada los registros de cualquier hallazgo que haya aceptado en lugar de corregir.

Detenerse en la primera corrección. Shellshock necesitó un segundo ID porque el primer parche dejó abierta una parte del fallo. Lea la descripción y las referencias de cada registro para encontrar ID posteriores y cierre un hallazgo solo cuando estén resueltos todos los ID que mencionan el componente.

Interpretar la ausencia de CVE como ausencia de vulnerabilidad. CVE cubre vulnerabilidades divulgadas públicamente y a las que una CNA ha asignado un ID dentro de su ámbito. Un fallo de su propio código no tiene CVE hasta que alguien lo notifica y lo publica. Comparar las dependencias con la lista cubre lo que otros han encontrado; su propio código necesita su propio análisis estático, revisión y pruebas.

Lecturas adicionales

- Programa CVE: descripción general — la misión, el registro CVE y los socios que los asignan y publican.
- Programa CVE: proceso — el formato del ID, el contenido mínimo de un registro y sus tres estados.
- Programa CVE: iniciativas relacionadas — cómo se relacionan NVD, CVSS, el catálogo KEV y CWE con CVE y en qué se diferencian.
- Common Vulnerability Scoring System v4.0: documento de especificación — los grupos de métricas de FIRST, las etiquetas de puntuación y la escala cualitativa de gravedad.

- CVE Record Format — la definición JSON de la estructura de un registro, en la versión que utiliza CVE Services.

- Programa CVE: preguntas frecuentes (archivo)

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es CVE?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/cve/