csurface

INFORME DE TELEMETRÍA · THREATSENSOR

El reloj del exploit

Cuánto tiempo hay entre la publicación de una CVE y el código que la explota, medido en la telemetría pública de ThreatSensor. Y por qué la cola ordenada por score llega después.

CVE EN LA BASE MONITOREADA	FABRICANTES ALCANZADOS	MEDICIÓN
928	225	17/sep/2026

CLASIFICACIÓN	FUENTE	VERIFICABLE
Público	csurface.io/threatsensor	Base abierta, sin registro

RESUMEN EJECUTIVO

Lo que decide, en una página

Esta página cierra sola. Quien lea solo esta página no se pierde ninguna decisión del informe.

Medido el 17/sep/2026
CSURFACE · ThreatSensor

MEDIANA HASTA EL PRIMER EXPLOIT PÚBLICO

1 día

la Cloud Security Alliance estimaba cinco en 2023

EPSS EN LA VÍSPERA DE ENTRAR AL KEV

0%

mediana de las 50 entradas más recientes de CISA

PLAZO MEDIANO QUE CONCEDE CISA

21 días

el mercado tarda 43 en corregir, según el DBIR 2026

Este informe corre sobre una base propia y pública: las **928 CVE** que ThreatSensor monitorea porque ya cargan señal de explotación. La base es abierta, no pide registro, y cualquier número de aquí se puede comprobar en la fuente.

Primero: el exploit llega antes que el plan. La mediana entre la publicación de una CVE y el primer exploit público de la base es de un día. En el 56,5% de los casos con esa medida disponible, el código ya existía el día de la publicación. Por la medida más conservadora, la de explotación observada, son 21,4%, cifra que queda en la misma franja del 28,96% que VulnCheck reportó en enero de 2026.

Segundo: ordenar por score llega tarde. En las cincuenta CVE más recientes en entrar al catálogo de explotación conocida de CISA, el EPSS mediano en la víspera de la entrada era cero. Y 450 de las 917 CVE bajo explotación observada en la base tienen CVSS por debajo de 9, o sea, no están arriba en ninguna cola ordenada por gravedad.

Tercero: el plazo regulatorio es más rápido que la práctica. CISA concede 21 días de mediana, y en 96 casos concedió tres. El DBIR 2026 mide 43 días de mediana para corregir, con apenas el 26% del catálogo de CISA totalmente cerrado.

Cuarto: no hay un fabricante en el cual concentrarse. Las 928 CVE alcanzan 502 productos de 225 fabricantes. Los seis mayores responden por un tercio de la base, y el resto es cola larga. Un programa que sigue boletines de fabricante cubre la parte fácil del problema.

Los cuatro convergen en una conclusión de cadencia, no de herramienta. Un ciclo de siete o de treinta días describe un estado que cambió antes de que el informe fuera abierto. Lo que mueve el resultado es disparar la verificación por evento, y llegar al equipo de corrección con decenas de elementos con evidencia en lugar de miles con una nota.

Qué hacer con esto el lunes. Levante tres números de su propio programa: cuántas horas pasan entre que una CVE gana explotación observada y su parque vuelve a ser examinado para ella; qué fracción de los hallazgos del último trimestre pasó por verificación de explotabilidad; y cuál es la mediana de horas entre que un activo queda expuesto y el equipo se entera. Los tres caben en una tarde y dicen más que cualquier conteo de hallazgos abiertos.

La base de este informe

CVE monitoreadas	**928**
En el catálogo KEV de CISA	**895**
Con exploit conocido	**261**
Con prueba de concepto pública	**557**
Ligadas a campaña de ransomware	**367**
Productos distintos alcanzados	**502**

Léala con esta salvedad: la base es curada y se inclina hacia el KEV, que responde por el 96% de ella. No representa el universo de CVE publicadas. Representa el recorte que ya tiene señal de explotación, y todo porcentaje de este informe es sobre ese recorte.

PARTE 01

El exploit dejó de esperar la divulgación

Dos medidas de tiempo, porque no coinciden y la diferencia entre ellas es información.

Medido el 17/sep/2026
CSURFACE · ThreatSensor

EXPLOIT PÚBLICO EXISTIENDO

56,5%

de las CVE con esa medida ya tenían código público de ataque el día en que fueron publicadas

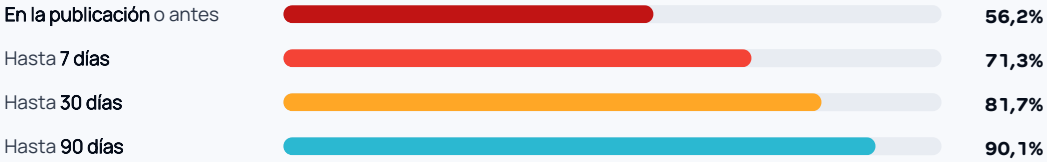
contra

EXPLOTACIÓN OBSERVADA

21,4%

ya estaban siendo explotadas en la fecha de publicación, por el criterio más estrecho

Cuánto tiempo hasta el primer exploit público (568 CVE)



Mediana de menos medio día. Restringiendo a las CVE publicadas en los últimos doce meses, la porción que ya tenía exploit en la publicación sube al 62,4%.

Por qué las dos medidas no coinciden. La primera cuenta la existencia de código público, incluyendo repositorio de prueba de concepto en GitHub, módulo de Metasploit y entrada en ExploitDB. La segunda cuenta evidencia de explotación observada, vía catálogo de CISA y sightings de CIRCL. El código publicado aparece antes de que alguien registre su uso, y por eso la primera medida siempre es mayor. El programa que planifica por la segunda planifica por lo que ya se vio ocurrir.

La serie por año de publicación de la CVE

AÑO	PUBLICADAS EN EL NVD	EXPLOTADA EN HASTA 5 DÍAS	YA EXPLOTADA EN LA PUBLICACIÓN
2020	21.076	43,6%	41,8%
2021	23.468	29,1%	27,2%
2022	27.554	31,6%	28,4%
2023	31.442	39,3%	28,7%
2024	39.247	32,3%	26,0%
2025	45.277	40,8%	24,2%
2026	**60.221**	**62,0%**	**52,4%**

Porcentajes sobre las CVE que ThreatSensor monitorea en cada año, no sobre el total publicado. El volumen del NVD es el conteo del año entero, excepto 2026, que llega hasta la fecha de la medición.

Lea 2026 con descuento. Es un año en curso, y una CVE publicada hace poco todavía no tuvo tiempo de acumular explotación tardía. Los dos efectos empujan hacia arriba la porción de casos que parecen haber sido explotados de inmediato. El salto respecto de los años anteriores sigue siendo grande después de descontar eso, pero no debe leerse como una cifra cerrada.

PARTE 02

La cola ordenada por score llega después del ataque

Lo que decían el EPSS y el CVSS sobre esas CVE en la víspera de su entrada al catálogo de explotación conocida.

Medido el 17/sep/2026
CSURFACE · ThreatSensor

EPSS MEDIANO EN LA VÍSPERA DEL KEV

0%

50 entradas más recientes; 86% por debajo del 1%

BAJO EXPLOTACIÓN CON CVSS POR DEBAJO DE 9

450

de 917 con nota asignada; 97 son media o baja

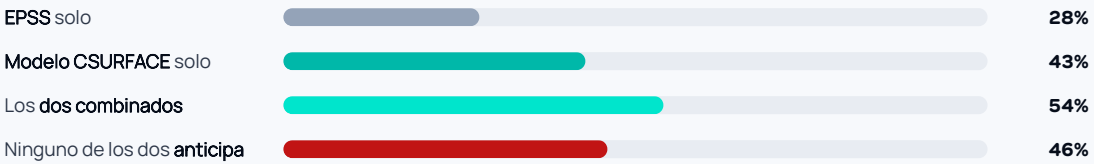
EN EL KEV CON EPSS POR DEBAJO DEL 10%

18,6%

166 de 894 CVE del catálogo

Backtest: qué señal anticipa la entrada al catálogo de CISA

Recorte temporal de validación desde 2024, con **82 CVE** que entraron al KEV en el período. La pregunta: cuántas de ellas pondría cada señal en su top 10% antes de que CISA las listara.



El modelo estima la probabilidad de que la CVE entre al KEV en 180 días y se entrena sin usar el EPSS como entrada, a propósito, para que las dos señales sigan siendo complementarias. El 46% que ninguna de las dos atrapa está publicado junto con el resto, porque un backtest que solo muestra aciertos no sirve para decidir nada.

Dónde se concentra la explotación

FABRICANTE	CVE	CVSS MEDIO
Microsoft	**100**	8,0
Google	**65**	8,8
Apple	**44**	8,5
Cisco	**41**	8,6
Ivanti	**33**	8,5
Apache	**26**	9,3

Los seis mayores responden por el 33% de la base. El resto se reparte en 502 productos y 225 fabricantes, que es la razón por la que ningún inventario por fabricante da cuenta del problema.

Qué significa esto para la cola. Un score sirve para ordenar, no para descubrir. Mientras la CVE no tiene señal pública, su EPSS es bajo por construcción, y queda al final de cualquier lista. Cuando la señal aparece, el score sube y la lista se reordena, solo que a esa altura la explotación ya empezó. La priorización por score necesita una segunda señal que mire lo que todavía no ocurrió.

PARTE 03

El plazo del regulador es la mitad del plazo practicado

Lo que CISA concede para corregir, lo que el mercado tarda, y el tamaño de la diferencia.

Medido el 17/sep/2026
CSURFACE · ThreatSensor

PLAZO CONCEDIDO POR CISA

21

días de mediana entre entrar al catálogo y vencer el plazo, en las 895 CVE del KEV en la base

contra

PLAZO QUE PRACTICA EL MERCADO

43

días de mediana para corregir, según el DBIR 2026 de Verizon, contra 32 el año anterior

Distribución de los plazos concedidos

21 días (estándar)	**502**
14 días	**161**
3 días (urgencia)	**96**
181 días (fin de vida)	**89**

En 96 casos CISA dio tres días. El plazo más corto de la base es de un día. La institución que trabaja en ciclo mensual descubre esos casos después de que el plazo ya venció.

El agravante del ransomware. De las 928 CVE monitoreadas, **367** tienen vínculo registrado con campaña de ransomware. No es un subconjunto exótico de la base: es más de un tercio de ella, y es la parte donde el intervalo entre explotación e impacto financiero se mide en horas y no en ciclos de corrección.

Lo que midieron otras fuentes en el mismo período

Corrección completa del catálogo de CISA — DBIR 2026	**26%**
CVE con primera evidencia de explotación en 2025 — VulnCheck	**884**
Fabricantes alcanzados por esas CVE — VulnCheck	**518**
Catalogadas por CISA en el mismo período — VulnCheck	**245**
Previsión de CVE publicadas en 2026 — FIRST	**66 mil**
Publicadas hasta la fecha de esta medición — NVD	**60.221**

La dispersión de nuestra base (502 productos, 225 fabricantes) y la de VulnCheck (672 productos, 518 fabricantes) son mediciones independientes del mismo orden de magnitud, lo que es una buena señal para las dos.

La cuenta que queda. Entre las 66 mil CVE previstas para el año y las pocas centenas con explotación observada hay dos órdenes de magnitud. Esa distancia es el trabajo de la priorización, y no se atraviesa con más escaneo. Se atraviesa con evidencia de que el camino existe en ese activo.

METODOLOGÍA Y LÍMITES

Cómo rehacer estos números, y lo que no dicen

Cada afirmación de este informe sale de una base abierta. Esta página existe para que pueda ser refutada.

Medido el 17/sep/2026
CSURFACE · ThreatSensor

Definiciones que cambian la lectura

Tiempo hasta el exploit público. Diferencia entre la fecha del primer artefacto público conocido y la fecha de publicación de la CVE. Artefacto incluye repositorio de prueba de concepto en GitHub, módulo de Metasploit y entrada en ExploitDB. Un valor negativo quiere decir que el artefacto ya existía cuando salió la CVE.

Tiempo hasta explotación observada. La misma cuenta contra la primera evidencia de uso registrado, vía catálogo de CISA y sightings de CIRCL. Es la medida conservadora, y la comparable con lo que publica VulnCheck.

La base es curada. Son 928 CVE, 895 de ellas en el KEV. No es una muestra del universo de CVE publicadas. Es el recorte que ya tiene señal de explotación, y todo porcentaje de este informe es sobre él.

La cola está sucia y fue tratada. La fecha de creación de un repositorio en GitHub a veces antecede a la CVE por años, porque el repositorio fue reutilizado. El caso extremo de la base marca menos 4.039 días. Por eso el informe reporta mediana y franjas, no promedio, y los agregados publicados en la página de analytics quitan outliers por rango intercuartil.

De dónde sale cada número

Base de CVE monitoreadas	**API pública de ThreatSensor**
Embudo por año de publicación	**Endpoint de embudo anual**
EPSS en la víspera del KEV, backtest	**Página de analytics**
Corrección mediana, catálogo CISA	**DBIR 2026, Verizon**
Explotación observada en 2025	**State of Exploitation 2026, VulnCheck**
Ventana de exploit histórica	**Cloud Security Alliance, abr/2026**
Previsión de volumen	**FIRST, jun/2026**

Compruébelo usted mismo. La base está abierta en csurface.io/threatsensor, sin registro y sin límite de consulta. Los agregados están en la página de analytics, que además explica cómo se construyó cada gráfico. Si un número de este informe no coincide con lo que usted mida, el error es nuestro y queremos saberlo.

Lo que este informe no es. No mide el parque de ningún cliente, no proyecta riesgo individual y no debe leerse como promesa de cobertura. Es la medición de un fenómeno de mercado sobre una base pública, hecha para sostener una decisión de cadencia y no para describir un producto.

csurface

SUPERFICIE EXTERNA · EVIDENCIA AUDITABLE

La pregunta dejó de ser cuántas CVE tiene. Es cuáles explota un atacante desde afuera.

CSURFACE audita la cobertura del escáner que la institución ya paga y prueba, con la evidencia que devuelve el propio objetivo, qué es explotable en la superficie externa. ThreatSensor, que produjo los números de este informe, es público y gratuito, y sigue así.

Descubrimiento de la superficie externa

Mapea lo que responde en internet a partir del dominio raíz, incluyendo el activo de la subsidiaria y lo que entró en una adquisición. Sin agente y sin lista que aportar.

Evidencia que devuelve el objetivo

Cada hallazgo llega con la evidencia que lo sostuvo y un grado de confianza explícito. Cuando la única forma de comprobar sería tirar el servicio, el elemento queda como probable.

Priorización por riesgo observado

La cola se ordena por señal de explotación en curso y no por gravedad teórica. Es la aplicación directa de lo que muestran las páginas 3 y 4 de este informe.

¿Quiere ver este retrato aplicado a su superficie?

Recibir el análisis preliminar de mi empresa →