csurface

RELATÓRIO DE TELEMETRIA · THREATSENSOR

O relógio do exploit

Quanto tempo existe entre a publicação de uma CVE e o código que a explora, medido na telemetria pública do ThreatSensor. E por que a fila ordenada por score chega depois.

CVES NA BASE MONITORADA	FORNECEDORES ATINGIDOS	APURAÇÃO
928	225	17/set/2026

CLASSIFICAÇÃO	FONTE	VERIFICÁVEL
Público	csurface.io/threatsensor	Base aberta, sem cadastro

O que decide, em uma página

Esta página fecha sozinha. Quem ler só ela não perde nenhuma decisão do relatório.

Apurado em 17/set/2026
CSURFACE · ThreatSensor

MEDIANA ATÉ O PRIMEIRO EXPLOIT PÚBLICO
1 dia
a Cloud Security Alliance estimava cinco em 2023

EPSS NA VÉSPERA DE ENTRAR NO KEV
0%
mediana das 50 entradas mais recentes da CISA

PRAZO MEDIANO QUE A CISA CONCEDE
21 dias
o mercado leva 43 para corrigir, segundo o DBIR 2026

Este relatório usa uma base própria e pública: as **928 CVEs** que o ThreatSensor monitora por já carregarem sinal de exploração. A base é aberta, não pede cadastro, e qualquer número aqui pode ser conferido na fonte.

Primeiro: o exploit chega antes do plano. A mediana entre a publicação de uma CVE e o primeiro exploit público na base é de um dia. Em 56,5% dos casos com essa medida disponível, o código já existia no dia da publicação. Pela medida mais conservadora, a de exploração observada, são 21,4%, número que fica na mesma faixa dos 28,96% que a VulnCheck reportou em janeiro de 2026.

Segundo: ordenar por score chega atrasado. Nas cinquenta CVEs mais recentes a entrar no catálogo de exploração conhecida da CISA, o EPSS mediano na véspera da entrada era zero. E 450 das 917 CVEs sob exploração observada na base têm CVSS abaixo de 9, ou seja, não estão no topo de nenhuma fila ordenada por gravidade.

Terceiro: o prazo regulatório é mais rápido que a prática. A CISA concede 21 dias de mediana, e em 96 casos concedeu três. O DBIR 2026 mede 43 dias de mediana para corrigir, com apenas 26% do catálogo da CISA totalmente fechado.

Quarto: não há fornecedor onde se concentrar. As 928 CVEs atingem 502 produtos de 225 fornecedores. Os seis maiores respondem por um terço da base, e o resto é cauda longa. Um programa que acompanha boletim de fabricante cobre a parte fácil do problema.

A conclusão para a qual os quatro convergem é de cadência, não de ferramenta. Ciclo de sete ou de trinta dias descreve um estado que mudou antes de o relatório ser aberto. O que muda o resultado é disparar a verificação por evento, e chegar ao time de correção com dezenas de itens com evidência no lugar de milhares com nota.

O que fazer com isso na segunda-feira. Levante três números do seu próprio programa: quantas horas passam entre uma CVE ganhar exploração observada e o seu parque ser reexaminado para ela; que fração dos achados do último trimestre passou por verificação de exploitabilidade; e qual a mediana de horas entre um ativo ficar exposto e o time saber. Os três cabem numa tarde e dizem mais que qualquer contagem de achados abertos.

Base deste relatório

CVEs monitoradas	**928**
No catálogo KEV da CISA	**895**
Com exploit conhecido	**261**
Com prova de conceito pública	**557**
Ligadas a campanha de ransomware	**367**
Produtos distintos atingidos	**502**

Leia com esta ressalva: a base é curada e puxa para o KEV, que responde por 96% dela. Ela não representa o universo de CVEs publicadas. Representa o recorte que já tem sinal de exploração, e todo percentual deste relatório é sobre esse recorte.

PARTE 01

O exploit deixou de esperar a divulgação

Duas medidas de tempo, porque elas discordam e a diferença entre as duas é informação.

Apurado em 17/set/2026
CSURFACE · ThreatSensor

EXPLOIT PÚBLICO EXISTINDO

56,5%

das CVEs com essa medida já tinham código público de ataque no dia em que foram publicadas

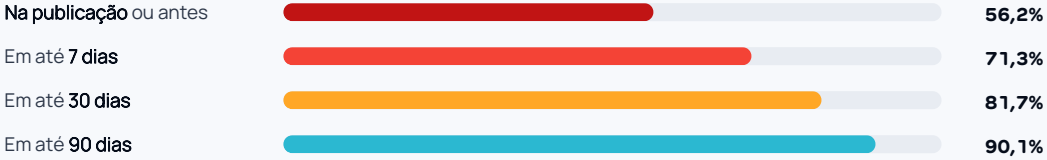
contra

EXPLORAÇÃO OBSERVADA

21,4%

já estavam sendo exploradas na data da publicação, pelo critério mais estreito

Quanto tempo até o primeiro exploit público (568 CVEs)



Mediana de menos meio dia. Restringindo às CVEs publicadas nos últimos doze meses, a fatia que já tinha exploit na publicação sobe para 62,4%.

Por que as duas medidas discordam. A primeira conta a existência de código público, incluindo repositório de prova de conceito no GitHub, módulo do Metasploit e entrada no ExploitDB. A segunda conta evidência de exploração observada, via catálogo da CISA e sightings do CIRCL. Código publicado aparece antes de alguém registrar o uso, e por isso a primeira medida é sempre maior. O programa que planeja pela segunda está planejando pelo que já foi visto acontecer.

A série por ano de publicação da CVE

ANO	PUBLICADAS NO NVD	EXPLORADA EM ATÉ 5 DIAS	JÁ EXPLORADA NA PUBLICAÇÃO
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%**

Percentuais sobre as CVEs que o ThreatSensor monitora em cada ano, não sobre o total publicado. O volume do NVD é a contagem do ano inteiro, exceto 2026, que vai até a data da apuração.

Leia 2026 com desconto. É ano em curso, e CVE publicada há pouco ainda não teve tempo de acumular exploração tardia. Os dois efeitos empurram para cima a fatia de casos que parecem ter sido explorados de imediato. A quebra em relação aos anos anteriores continua grande depois de descontar isso, mas ela não deve ser lida como um número fechado.

PARTE 02

A fila ordenada por score chega depois do ataque

O que o EPSS e o CVSS diziam sobre as CVEs na véspera de elas entrarem no catálogo de exploração conhecida.

Apurado em 17/set/2026
CSURFACE · ThreatSensor

EPSS MEDIANO NA VÉSPERA DO KEV

0%

50 entradas mais recentes; 86% abaixo de 1%

SOB EXPLORAÇÃO COM CVSS ABAIXO DE 9

450

de 917 com nota atribuída; 97 são média ou baixa

NO KEV COM EPSS ABAIXO DE 10%

18,6%

166 de 894 CVEs do catálogo

Backtest: quem antecipa a entrada no catálogo da CISA

Recorte temporal de validação a partir de 2024, com **82 CVEs** que entraram no KEV no período. A pergunta: quantas delas cada sinal colocaria no seu top 10% antes de a CISA listar.

O modelo estima a probabilidade de a CVE entrar no KEV em 180 dias e é treinado sem usar o EPSS como entrada, de propósito, para que os dois sinais permaneçam complementares. Os 46% que nenhum dos dois pega estão publicados junto com o resto, porque um backtest que só mostra acerto não serve para decidir nada.

Onde a exploração se concentra

FORNECEDOR	CVES	CVSS MÉDIO
Microsoft	**100**	8,0
Google	**65**	8,8
Apple	**44**	8,5
Cisco	**41**	8,6
Ivanti	**33**	8,5
Apache	**26**	9,3

Os seis maiores respondem por 33% da base. O restante se espalha por 502 produtos e 225 fornecedores, o que é a razão de nenhum inventário por fornecedor dar conta do problema.

O que isso significa para a fila. Um score serve para ordenar, não para descobrir. Enquanto a CVE não tem sinal público, o EPSS dela é baixo por construção, e ela fica no fim de qualquer lista. Quando o sinal aparece, o score sobe e a lista se reordena, só que a essa altura a exploração já começou. Priorização por score precisa de um segundo sinal que olhe para o que ainda não aconteceu.

PARTE 03

O prazo do regulador é metade do prazo da prática

O que a CISA concede para corrigir, o que o mercado leva, e o tamanho da diferença.

Apurado em 17/set/2026
CSURFACE · ThreatSensor

PRAZO CONCEDIDO PELA CISA

21

dias de mediana entre entrar no catálogo e vencer o prazo, nas 895 CVEs do KEV na base

contra

PRAZO PRATICADO PELO MERCADO

43

dias de mediana para corrigir, segundo o DBIR 2026 da Verizon, contra 32 no ano anterior

Distribuição dos prazos concedidos

21 dias (padrão)	**502**
14 dias	**161**
3 dias (urgência)	**96**
181 dias (fim de vida)	**89**

Em 96 casos a CISA deu três dias. O menor prazo da base é de um dia. A instituição que trabalha em ciclo mensal descobre esses casos depois de o prazo ter vencido.

O que outras fontes mediram no mesmo período

Correção completa do catálogo da CISA — DBIR 2026	**26%**
CVEs com primeira evidência de exploração em 2025 — VulnCheck	**884**
Fornecedores atingidos por essas CVEs — VulnCheck	**518**
Catalogadas pela CISA no mesmo período — VulnCheck	**245**
Previsão de CVEs publicadas em 2026 — FIRST	**66 mil**
Publicadas até a data desta apuração — NVD	**60.221**

A dispersão da nossa base (502 produtos, 225 fornecedores) e a da VulnCheck (672 produtos, 518 fornecedores) são apurações independentes na mesma ordem de grandeza, o que é um bom sinal para as duas.

O agravante do ransomware. Das 928 CVEs monitoradas, **367** têm ligação registrada com campanha de ransomware. Não é um subconjunto exótico da base: é mais de um terço dela, e é a parte em que o intervalo entre exploração e impacto financeiro se mede em horas, não em ciclos de correção.

A conta que sobra. Entre as 66 mil CVEs previstas para o ano e as poucas centenas com exploração observada há duas ordens de grandeza. Essa distância é o trabalho da priorização, e ela não se atravessa com mais varredura. Atravessa-se com evidência de que o caminho existe naquele ativo.

METODOLOGIA E LIMITES

Como refazer estes números, e o que eles não dizem

Cada afirmação deste relatório sai de uma base aberta. Esta página existe para que ela possa ser contestada.

Apurado em 17/set/2026
CSURFACE · ThreatSensor

Definições que mudam a leitura

Tempo até o exploit público. Diferença entre a data do primeiro artefato público conhecido e a data de publicação da CVE. Artefato inclui repositório de prova de conceito no GitHub, módulo do Metasploit e entrada no ExploitDB. Valor negativo quer dizer que o artefato já existia quando a CVE saiu.

Tempo até exploração observada. A mesma conta contra a primeira evidência de uso registrado, via catálogo da CISA e sightings do CIRCL. É a medida conservadora, e é a comparável com o que a VulnCheck publica.

A base é curada. São 928 CVEs, 895 delas no KEV. Não é amostra do universo de CVEs publicadas. É o recorte que já tem sinal de exploração, e todo percentual deste relatório é sobre ele.

A cauda é suja e foi tratada. A data de criação de um repositório no GitHub às vezes antecede a CVE por anos, porque o repositório foi reaproveitado. O caso extremo da base marca menos 4.039 dias. Por isso o relatório reporta mediana e faixas, não média, e os agregados publicados na página de analytics removem outlier por intervalo interquartil.

De onde vem cada número

Base de CVEs monitoradas	**API pública do ThreatSensor**
Funil por ano de publicação	**Endpoint de funil anual**
EPSS na véspera do KEV, backtest	**Página de analytics**
Correção mediana, catálogo CISA	**DBIR 2026, Verizon**
Exploração observada em 2025	**State of Exploitation 2026, VulnCheck**
Janela de exploit histórica	**Cloud Security Alliance, abr/2026**
Previsão de volume	**FIRST, jun/2026**

Confira você mesmo. A base está aberta em csurface.io/threatsensor, sem cadastro e sem limite de consulta. Os agregados estão na página de analytics, e a página traz a explicação de como cada gráfico foi construído. Se um número deste relatório não bater com o que você apurar, o erro é nosso e queremos saber.

O que este relatório não é. Ele não mede o parque de nenhum cliente, não projeta risco individual e não deve ser lido como promessa de cobertura. É a medição de um fenômeno de mercado numa base pública, feita para sustentar uma decisão de cadência, não para descrever um produto.

csurface

SUPERFÍCIE EXTERNA · EVIDÊNCIA AUDITÁVEL

A pergunta deixou de ser quantas CVEs você tem. É quais um atacante explora de fora.

A CSURFACE audita a cobertura do scanner que a instituição já paga e prova, com a evidência que o próprio alvo devolve, o que é explorável na superfície externa. O ThreatSensor, que produziu os números deste relatório, é público e gratuito, e continua assim.

Descoberta da superfície externa

Mapeia o que responde na internet a partir do domínio raiz, incluindo o ativo da subsidiária e o que entrou numa aquisição. Sem agente e sem lista a fornecer.

Evidência que o alvo devolve

Cada achado chega com a evidência que o sustentou e um grau de confiança explícito. Quando a única forma de comprovar seria derrubar o serviço, o item fica como provável.

Priorização por risco observado

A fila se ordena por sinal de exploração em curso, não por gravidade teórica. É a aplicação direta do que as páginas 3 e 4 deste relatório mostram.

Quer ver esse retrato aplicado à sua superfície?

Receber a análise preliminar da minha empresa →