QUOR
BY GETUP

O disclosure gap e seus efeitos em programas de segurança.

Publicação em **03 de julho de 2026**
Versão 1

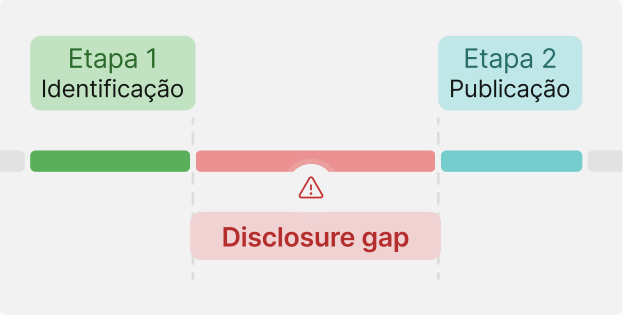
Sumário

A arquitetura de um programa de vulnerability management moderno é construída sobre rastreamento: scanners inspecionam imagens de container, pacotes de sistema e dependências de aplicação em busca de correspondências com bancos de dados de vulnerabilidades conhecidas, quando uma correspondência é encontrada, um identificador CVE é associado ao componente afetado, uma severidade é atribuída com base no CVSS, e o item entra no fluxo de remediação com um prazo definido. O processo é auditável, rastreável e, na maior parte das organizações maduras, automatizado.

> Essa estrutura funciona bem para o que ela mede. O problema é o que ela não mede.

O programa CVE, administrado pelo MITRE, formaliza o processo de registro de vulnerabilidades em duas etapas distintas:

1. Na primeira, um identificador é reservado para uma vulnerabilidade específica, geralmente no momento em que um pesquisador ou vendor inicia o processo de disclosure coordenado.
2. Na segunda, esse identificador é publicado, com detalhes técnicos, referências e metadados, tornando-se visível para o ecossistema.



Entre essas duas etapas existe um intervalo de tempo durante o qual a vulnerabilidade já é conhecida por ao menos o pesquisador que a descobriu e o vendor responsável pelo componente afetado, mas ainda não tem existência pública. Scanners não a detectam, ferramentas de correlação não a indexam, logo, SLAs de remediação não são ativados. Para os sistemas que dependem de identificadores públicos como referência, o ambiente parece limpo.

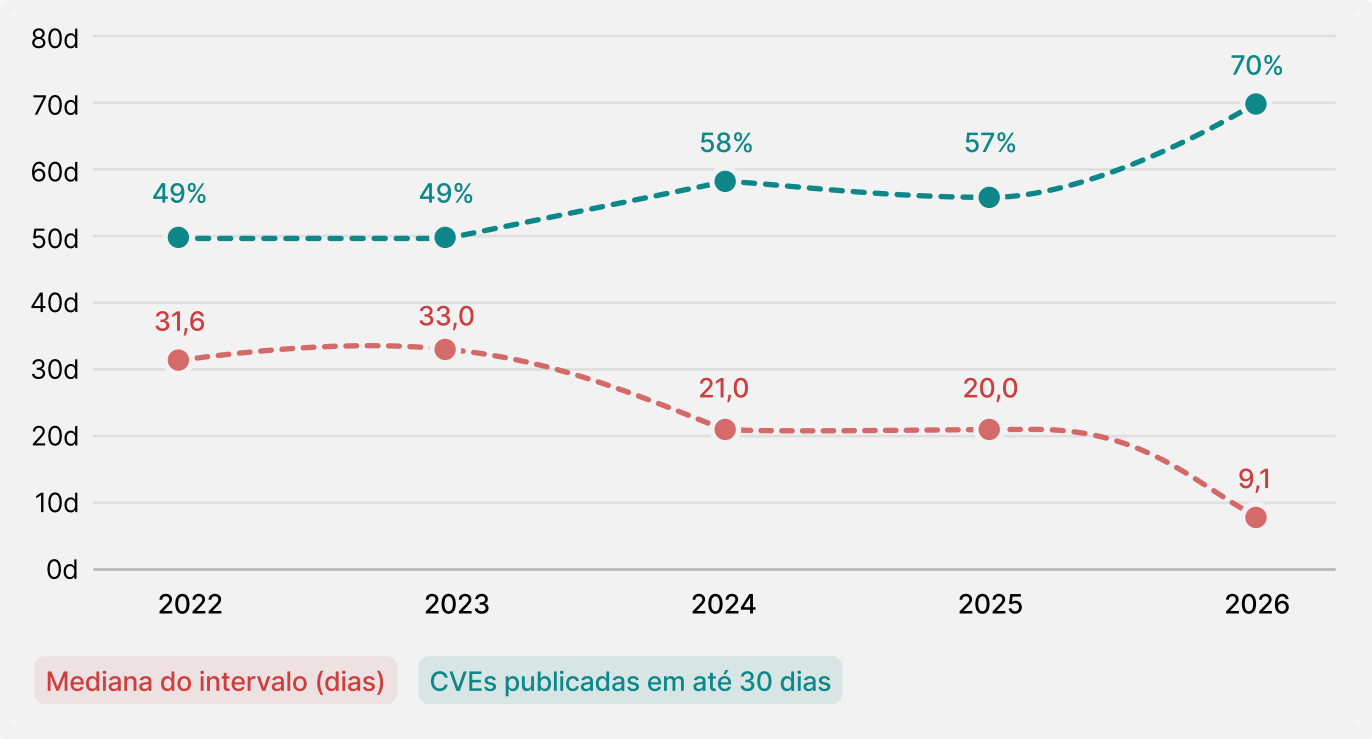
Esse intervalo é o que este report denomina de: **disclosure gap.**

A distinção importa porque o modelo de risco predominante trata a data de publicação da CVE como equivalente ao início da exposição. É a partir dessa data que se contam os dias de SLA, que se calcula o *Mean Time To Remediate* (MTTR) e que se avaliam programas de security posture em auditorias. Se a data de publicação sistematicamente ocorre semanas ou meses após a descoberta, então toda a estrutura de medição de risco está calibrada sobre um ponto temporal incorreto.

A potencial exposição começa antes, o quanto antes é exatamente o que esta pesquisa buscou quantificar.

Para isso, foram analisados 133.716 registros CVE publicados entre 2021 e 2026, extraídos do repositório público CVEListV5 [1], mantido pelo programa CVE/MITRE. O intervalo medido é o tempo entre o campo ***dateReserved***, que marca o momento da alocação do identificador, e o campo ***datePublished***, que marca a publicação. Esse intervalo representa um limite inferior do período de exposição real: a descoberta da vulnerabilidade precede a reserva do identificador, de modo que o gap efetivo é sempre maior do que o registrado nos metadados.

Os resultados mostram que o ecossistema melhorou de forma consistente ao longo do período. A mediana do intervalo caiu de **31,6 dias em 2022** para **9,1 dias em 2026**, uma **redução de 71%**. A proporção de **CVEs publicadas em até 30 dias cresceu de 49% para 70%** no mesmo período. Essa melhora é real e relevante. Ela não elimina, porém, o problema estrutural: mesmo **em 2026, 30% das CVEs levaram mais de 30 dias para se tornar visíveis**. Para determinadas classes de vulnerabilidade, o intervalo típico ultrapassa 40 dias. E para as vulnerabilidades presentes no catálogo CISA KEV, aquelas com exploração confirmada in-the-wild, a mediana no período (2021–2026) é de 31 dias, acima da população geral.



As seções seguintes detalham o que determina o tamanho desse intervalo, como ele se distribui por tipo de vulnerabilidade e severidade, e o que suas implicações concretas significam para programas de vulnerability management.

Disclosure gap em detalhes

O processo de disclosure coordenado de vulnerabilidades parte de uma lógica de proteção coletiva: o pesquisador que descobre uma falha notifica o vendor antes de torná-la pública, concedendo tempo para que uma correção seja desenvolvida e distribuída. Esse modelo é o padrão predominante no ecossistema e a base sobre a qual o programa CVE opera.

O fluxo envolve etapas sequenciais: descoberta, report privado ao fabricante, confirmação, desenvolvimento da correção, release e publicação coordenada com o registro do identificador CVE. Cada etapa tem seu próprio tempo. Durante todo esse intervalo, a vulnerabilidade existe, é conhecida por ao menos duas partes, e não aparece em nenhum scanner, pois não há identificador público para correlacionar.

Essa é uma ausência de informação estrutural do dado no sistema.

Esse comportamento não é uma falha de implementação dos scanners. É uma consequência direta de como o sistema funciona: ferramentas de correlação de vulnerabilidades indexam o que é conhecido publicamente. O disclosure gap é, por definição, o período em que a vulnerabilidade ainda não é conhecida publicamente. Os dois conceitos são estruturalmente incompatíveis.

Vale distinguir o ***disclosure gap*** do ***patch gap***, conceito mais estabelecido. O patch gap descreve o tempo entre uma correção estar disponível e essa correção chegar ao ambiente de produção. Durante o patch gap, o problema é visível e o SLA está contando. Durante o disclosure gap, o problema não tem visibilidade e nenhum processo automatizado foi ativado.

O disclosure gap é a camada anterior, e é justamente por isso que raramente aparece em programas de vulnerability management.

O caso do IngressNightmare [2], em 2025, ilustra o problema em escala: uma vulnerabilidade no Ingress-NGINX Controller para Kubernetes, classificada com CVSS 9.8, descoberta pela Wiz, permaneceu em coordenação por 84 dias entre o report inicial e a publicação das CVEs. Segundo a própria Wiz, cerca de 43% dos ambientes cloud analisados estavam expostos. Durante todo esse período, nenhum scanner sinalizou nada. Ou seja, durante esse período, qualquer ator com conhecimento da vulnerabilidade tinha condições técnicas de explorá-la em quase metade dos ambientes cloud ativos.

Esse conhecimento não é necessariamente exclusivo do pesquisador e do vendor: processos de coordenação envolvem múltiplas partes, commits de correção ficam visíveis em repositórios públicos antes do disclosure formal, e inteligência de ameaças é um mercado. Os sistemas de segurança dessas organizações não sinalizaram nada porque não tinham base para isso. O intervalo não monitorado é exatamente esse.

O que nós analisamos

Para quantificar o disclosure gap de forma sistemática, foram analisados 133.716 registros CVE publicados entre 2021 e 2026, extraídos do repositório público CVEListV5, mantido pelo programa CVE/MITRE.

O intervalo medido é o tempo entre o campo dateReserved, que marca o momento da alocação do identificador, e o campo datePublished, que marca a publicação pública.

Registros sem um dos dois campos, com datas inválidas ou com lag negativo foram excluídos. O ano de 2021 apresenta apenas 237 registros, reflexo da adoção gradual do formato JSON v5, e foi tratado como atípico nas análises temporais.

A distribuição do intervalo tem três características que definem como os dados devem ser lidos:

1. A moda é zero em todos os anos analisados: publicação no mesmo dia da reserva é o valor mais frequente em qualquer subconjunto. Nesses casos a métrica não captura nada do período de coordenação. Ou seja, isso mostra que ***dateReserved*** é um proxy de descoberta, o intervalo medido é um limite inferior do gap real, a fração de "mesmo dia" reflete a prática de reserva em lote, não disclosure instantâneo.

2. Nos anos consolidados (2022–2025), a razão entre média e mediana fica entre 2 e 3,5 vezes, chegando a cerca de 4,5 em 2026 (ainda parcial), indicando uma cauda direita longa, com casos extremos que distorcem a média significativamente.

3. O maior intervalo registrado no dataset é de 4.741 dias, correspondente a uma CVE reservada em 2008 e publicada em 2021. Por essas razões, a mediana foi adotada como métrica principal ao longo desta análise.

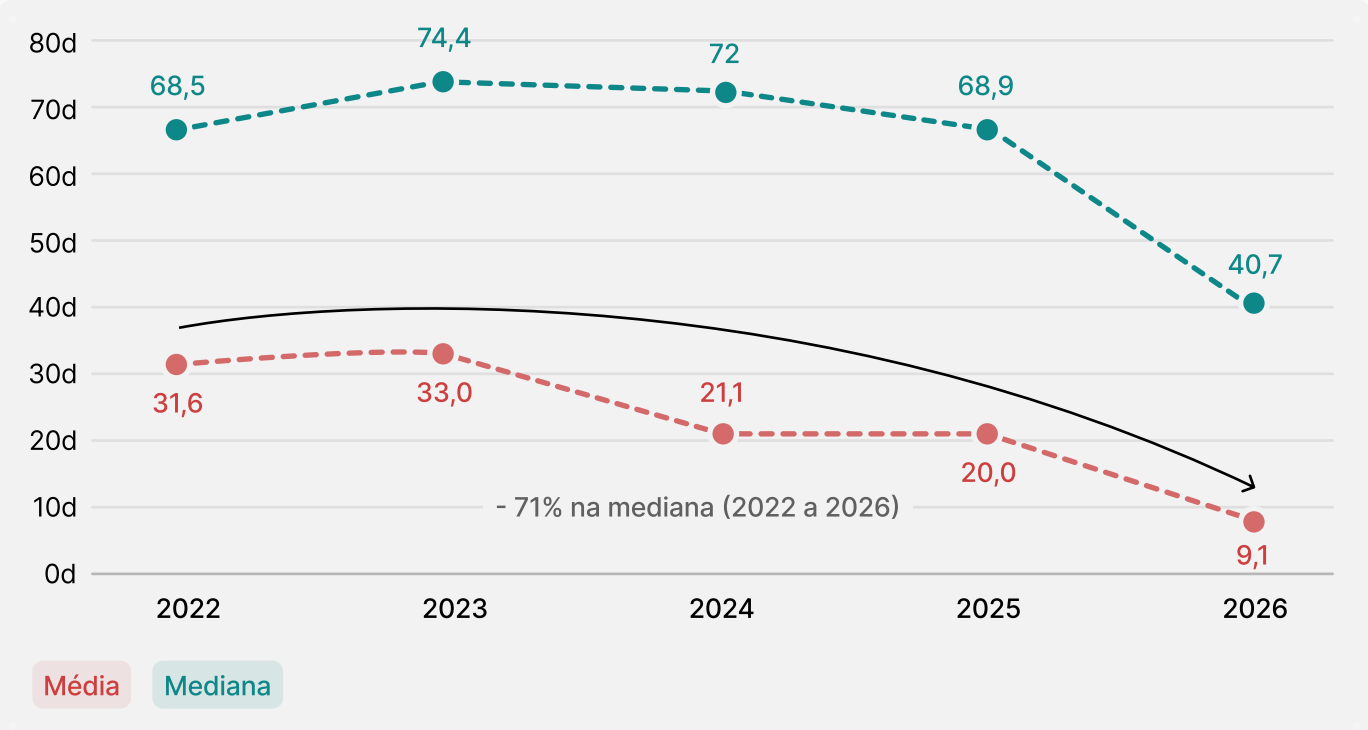
A tendência central do período é de redução.

- A mediana caiu de 31,6 dias em 2022, para 9,1 dias em 2026, uma queda de 71% em quatro anos.
- A proporção de CVEs publicadas em até 30 dias cresceu de 49% para 70% no mesmo período.

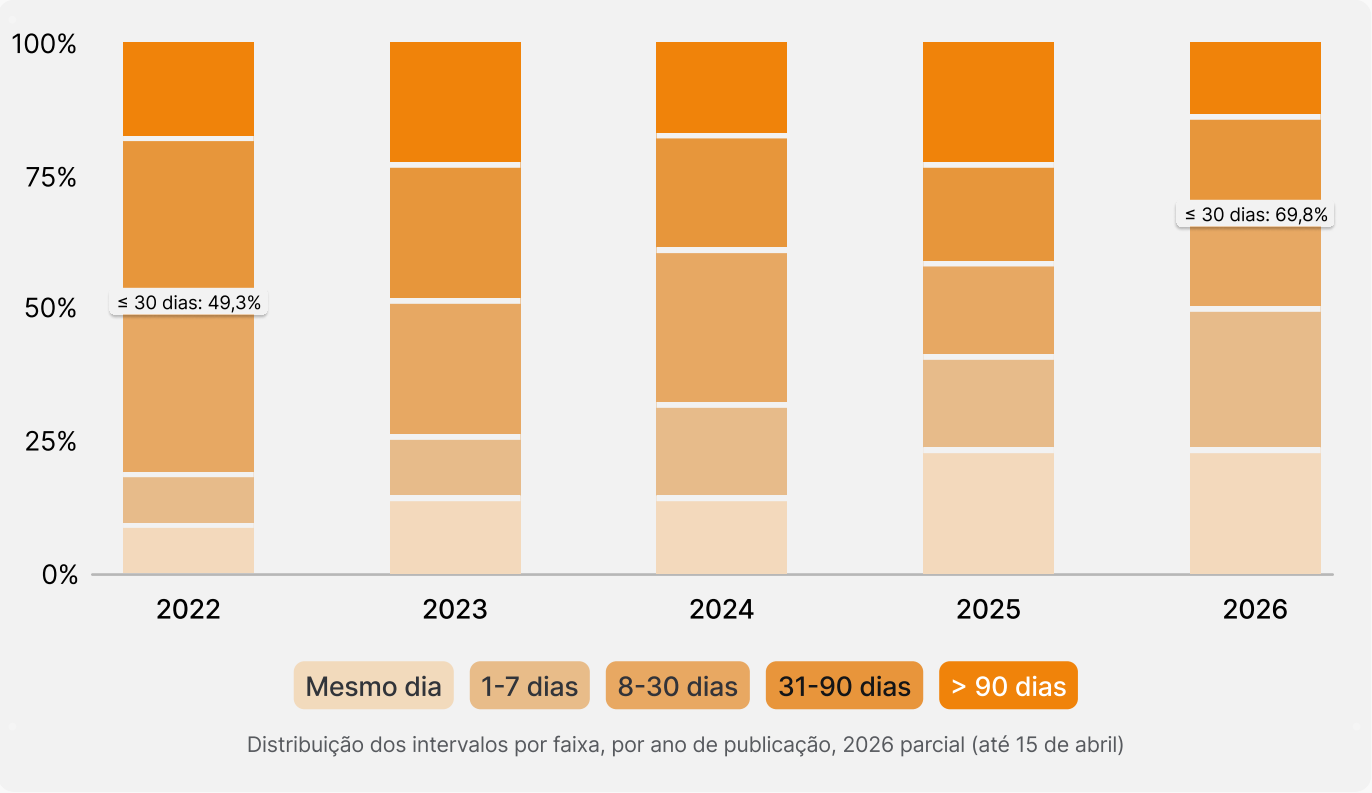
Essa melhora reflete maior maturidade operacional dos CNAs, adoção crescente de processos estruturados de disclosure e, possivelmente, pressão regulatória e de mercado sobre vendors para reduzir o tempo de resposta.

Ano	Mediana	Média	Mesmo dia	Até 7 dias	Até 30 dias	Acima de 1 ano
2022	31,6 dias	68,5 dias	9,1%	19,1%	49,2%	1,4%
2023	33,0 dias	74,4 dias	14,1%	24,8%	48,6%	1,9%
2024	21,0 dias	71,9 dias	14,8%	30,9%	58,1%	3,0%
2025	20,0 dias	68,9 dias	23,1%	38,9%	57,4%	3,0%
2026	9,0 dias	40,3 dias	22,2%	48,4%	70,3%	1,1%

O intervalo mediano entre reserva e publicação caiu 71% em quatro anos



A publicação migra para janerlas curtas: a fração ≤30 dias sobe de 49% para 70%



Distribuição dos intervalos por faixa, por ano de publicação, 2026 parcial (até 15 de abril)

A distância persistente entre média e mediana merece atenção: em 2025, a mediana foi de 20 dias e a média de 68,9 dias, uma diferença de 3,4 vezes. Isso significa que a maior parte das CVEs é publicada rapidamente, mas uma parcela relevante leva meses, puxando a média para cima. Programas de segurança que utilizam médias do setor como referência para avaliar sua postura estão trabalhando com um número sistematicamente inflado pelo comportamento de uma minoria de casos. A mediana representa melhor o comportamento típico do ecossistema.

Um dado que merece destaque é o comportamento da cauda longa: em 2024 e 2025, 3% das CVEs levaram mais de um ano para ser publicadas após a reserva do identificador. Esse grupo é composto majoritariamente por registros retroativos do MITRE para software legado, plugins catalogados com atraso sistemático e firmware de hardware com ciclos de patch semestrais. Apenas 0,1% dessas CVEs com lag superior a um ano estão presentes no catálogo CISA KEV, e metade tem severidade MEDIUM. A cauda longa existe, mas não representa concentração de risco crítico.

O que os dados estabelecem, em conjunto, é que o disclosure gap é um fenômeno mensurável, com magnitude e distribuição conhecidas. A seção seguinte examina o que determina o tamanho desse intervalo para diferentes tipos de vulnerabilidade.

QUOR
BY GETUP

3

O que determina o tamanho do gap

Uma vez estabelecida a existência e a magnitude do disclosure gap, como discutido na seção **"O que nós analisamos"**, a pergunta relevante para quem define política de segurança é: **"quais vulnerabilidades ficam mais tempo fora do registro público?"**

A resposta tem implicações diretas sobre quais componentes de um ambiente representam maior exposição durante o intervalo não monitorado.

A análise testou duas categorias de fatores:

1. O tipo de vulnerabilidade, classificado pelo CWE;
2. Os atributos de severidade do CVSS v3.x.

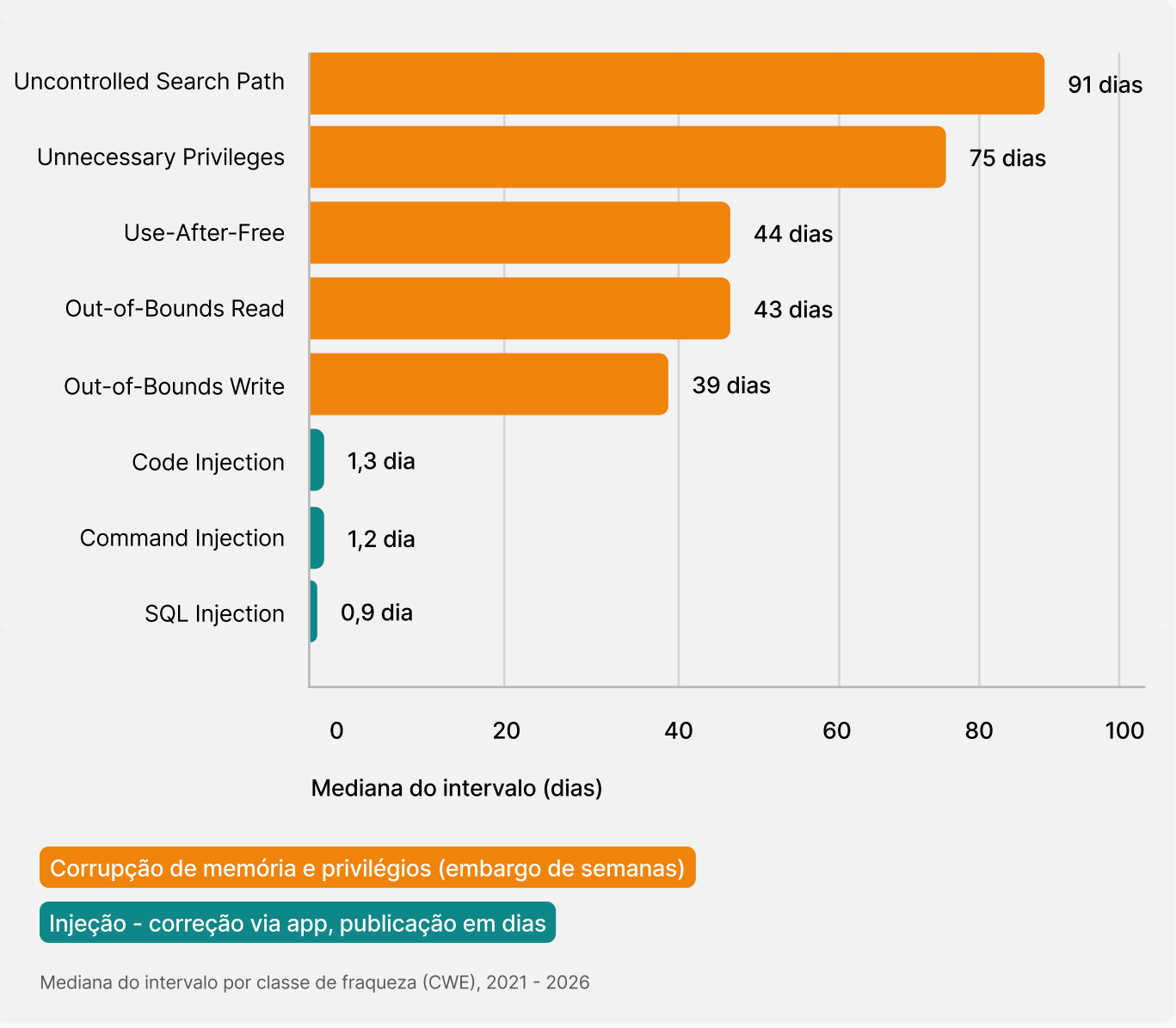
Os resultados são assimétricos de forma relevante.

O tipo de vulnerabilidade é o fator que mais determina o tamanho do gap, com margem considerável sobre os demais.

A severidade, medida pelo CVSS, tem influência pequena. Saber que uma vulnerabilidade é crítica diz pouco sobre quanto tempo ela ficará fora do registro público.

Saber que ela é uma vulnerabilidade de corrupção de memória diz muito mais.

O tipo de vulnerabilidade decide o gap - mais que a severidade



Mediana do intervalo por classe de fraqueza (CWE), 2021 - 2026

Vulnerabilidades de injeção, como SQL Injection e Code Injection, têm mediana de publicação abaixo de 2 dias porque suas correções são deployadas via atualização de aplicação, sem recompilação de binários ou ciclos de distribuição via gerenciadores de pacotes. O processo de disclosure pode ser concluído rapidamente porque a cadeia de distribuição de correção é curta.

Vulnerabilidades de corrupção de memória e escalonamento de privilégios seguem o padrão oposto. Use-After-Free tem mediana de 44 dias, Out-of-Bounds Read, 43 dias, Uncontrolled Search Path, 91 dias. Correções nessas classes exigem compilação de binários, testes extensivos de regressão e distribuição via gerenciadores de pacotes, um processo que leva semanas independentemente da urgência declarada.

A diferença entre os extremos supera 50 vezes. Uma vulnerabilidade crítica pode ter intervalo de publicação curto ou longo dependendo de sua classe técnica, não de sua severidade. O CVSS não captura essa distinção.

O vetor de ataque é o atributo CVSS com maior variação observada: vulnerabilidades com vetor de rede têm mediana de 28,5 dias, enquanto vulnerabilidades com vetor físico chegam a 73,9 dias. O gradiente é consistente, mas o poder explicativo continua modesto. Severidade, impacto em confidencialidade e disponibilidade apresentam variações ainda menores entre seus valores extremos.

A implicação prática seria: em ambientes que utilizam componentes de sistema operacional, bibliotecas de baixo nível e dependências compiladas, a exposição ao disclosure gap é estruturalmente maior.

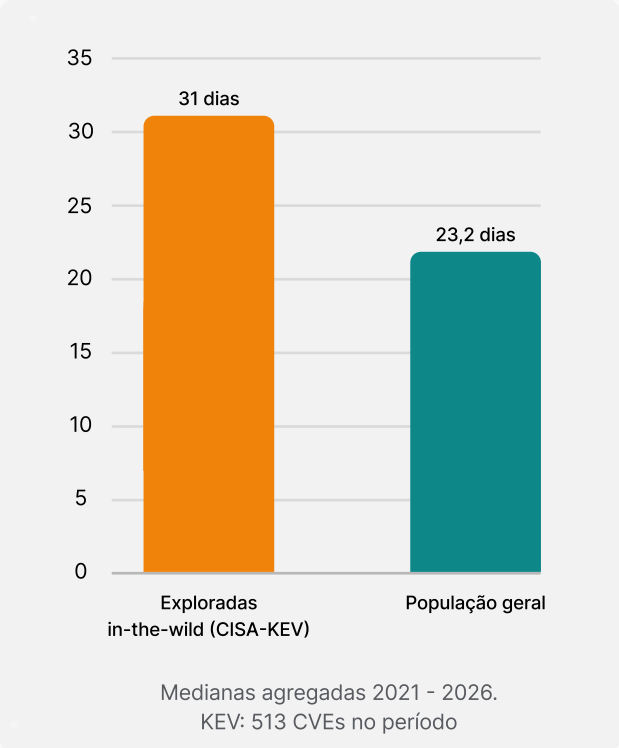
O tipo de componente presente no ambiente determina, em boa medida, o intervalo típico de exposição não monitorada ao qual esse ambiente está sujeito. Ambientes com maior concentração de componentes de infraestrutura e runtime ficam expostos por mais tempo, e essa exposição não aparece em nenhum dashboard de segurança enquanto o gap está aberto.

Vulnerabilidades exploradas in-the-wild

Uma suposição razoável, dado o modelo de risco predominante, seria a de que vulnerabilidades exploradas ativamente em ambientes reais fossem publicadas mais rapidamente. Se uma falha está sendo usada por atacantes, haveria incentivo para acelerar o disclosure e reduzir o tempo de exposição do ecossistema. Os dados não confirmam essa hipótese.

O catálogo CISA KEV, que reúne vulnerabilidades com exploração confirmada in-the-wild, foi cruzado com o dataset. Das 1.569 entradas do catálogo, 513 foram publicadas no período estudado (2021–2026) e têm intervalo disponível. Tomando esse período como um único conjunto, a mediana dessas CVEs do KEV é de 31 dias, contra 23,2 dias na população geral, dois valores agregados de todo o período, não de um ano específico.

Ou seja, vulnerabilidades exploradas ativamente levam, em mediana, mais tempo para serem publicadas, não menos.



Medianas agregadas 2021 - 2026.
KEV: 513 CVEs no período

As CVEs do KEV concentram-se em grandes vendors com processos formais de disclosure: Microsoft, Apple, Google e Adobe respondem pelos principais atribuidores do catálogo.

Esses vendors operam ciclos estruturados de publicação, como o Patch Tuesday da Microsoft, que agrupa correções em datas fixas independentemente de quando cada vulnerabilidade foi descoberta ou confirmada. O lag maior é consequência de processos mais elaborados de coordenação, não de menor urgência percebida.

O perfil de severidade do KEV reforça a relevância do catálogo para programas de segurança. Cerca de 86% das CVEs do KEV têm CVSS igual ou superior a 7,0 e 39% são classificadas como críticas, contra aproximadamente 44% e 10%, respectivamente, na população geral. As classes de vulnerabilidade dominantes são de: execução remota de código e Insecure Deserialization.

O que os dados estabelecem é que o disclosure gap afeta de forma pronunciada exatamente as vulnerabilidades que mais importam para um programa de segurança. Não se trata de um intervalo concentrado em falhas de baixa severidade ou em software de nicho. As vulnerabilidades com maior probabilidade de exploração real são as mesmas que ficam mais tempo fora do registro público, com uma mediana no periodo de 31 dias.

QUOR
BY GETUP

5

O que seus SLAs não medem

Programas de vulnerability management estruturados em torno de SLAs por severidade têm uma utilidade operacional clara: definem prazos, criam accountability e permitem auditoria.

O problema é a referência temporal sobre a qual eles operam:

1. O *clock* do SLA começa na data de publicação da CVE, essa data é o momento em que o identificador se torna público no NVD ou em fontes equivalentes, e é a partir dela que scanners detectam a vulnerabilidade, ferramentas de correlação a indexam e equipes de remediação são acionadas. Para fins operacionais, é uma referência conveniente porque é objetiva, rastreável e padronizada.
2. O que ela não representa é o início da exposição. A exposição começa no momento da descoberta, que precede a reserva do identificador, que por sua vez precede a publicação. O SLA mede o tempo de resposta a partir de um ponto que já está no meio, ou no fim, do período de risco real. O *Mean Time To Remediate* calculado sobre essa referência é uma métrica de eficiência operacional, não uma medida de exposição acumulada.

As consequências práticas são três:

- Auditorias de segurança realizadas durante o disclosure gap não encontram apontamentos porque os scanners não têm base para reportar nada.
- Métricas de MTTR ficam sistematicamente subestimadas porque o período anterior à publicação não é contabilizado.
- E SLAs de remediação não são ativados para vulnerabilidades que já existem no ambiente, são conhecidas por vendors e pesquisadores, e em alguns casos podem já estar sendo exploradas.

O State of the Software Supply Chain 2026, da Sonatype, documentou que em 2025 o tempo mediano do NVD para atribuir um CVSS score a uma CVE após sua publicação foi de 41 dias. Isso significa que, além do disclosure gap anterior à publicação, existe um segundo intervalo entre a publicação da CVE e o enriquecimento com metadados de severidade que muitas ferramentas utilizam para priorização.

Os dois intervalos se somam. Uma vulnerabilidade pode ser descoberta, ter seu identificador reservado, ser publicada sem score e só então receber uma classificação de severidade semanas depois. Durante todo esse trajeto, o SLA baseado em severidade não foi ativado uma única vez.

O disclosure gap invalida a suposição de que os SLAs cobrem o período de exposição completo. Para organizações que utilizam métricas de segurança para tomar decisões sobre postura e investimento, essa distinção tem implicações diretas sobre a qualidade da informação disponível.

Opinião do Especialista

Não há o que uma empresa faça sobre o disclosure gap. Ele é do ecossistema, não nosso. O que sobra é o que sempre esteve na nossa mão: reduzir a superfície, escolher componente com critério, parar de medir exposição como se a janela não existisse. Nada disso é novo. O gap só não nos deixa mais adiar.

Diogo Goebel
CEO Getup

Recomendações práticas

O disclosure gap não é um problema com solução única, ele é consequência de como o ecossistema de segurança funciona: descoberta privada, coordenação entre partes, publicação coordenada. Esse modelo existe por razões legítimas e não será substituído. O que organizações podem fazer é ajustar seus programas de segurança para operar com consciência do intervalo, em vez de ignorá-lo estruturalmente. As recomendações a seguir não pressupõem substituição de ferramentas ou reestruturação de processos. Pressupõe ajustes na forma como informação de vulnerabilidade é consumida e como risco é medido.

Monitorar fontes anteriores ao NVD:

O GitHub Security Advisories, o OSV.dev e os security channels dos projetos upstream frequentemente publicam informações antes do NVD processar e atribuir score. Ferramentas que consomem apenas o NVD estão sistematicamente atrasadas em relação a quem monitora o upstream diretamente. Para componentes críticos do ambiente, o monitoramento direto de repositórios e canais de segurança dos projetos reduz o intervalo entre a existência pública de um advisory e a ciência da equipe de segurança.

Distinguir ausência de CVE de ausência de risco:

a superfície de ataque de um sistema é definida pelo que existe no código, não pelo que os scanners conseguem correlacionar com um banco de dados de vulnerabilidades. Um componente sem CVE registrada pode estar em processo ativo de disclosure, pode ter uma correção disponível upstream ainda não empacotada pela distribuição, ou pode simplesmente nunca ter sido auditado. A ausência de alerta do scanner não é equivalente à ausência de exposição.

Reduzir a superfície de ataque estruturalmente:

o tamanho do disclosure gap varia por tipo de componente. Ambientes com maior concentração de bibliotecas de baixo nível, dependências compiladas e componentes de sistema operacional ficam expostos por intervalos maiores, como demonstrado na seção 4. Reduzir o número de componentes presentes no ambiente, utilizando imagens minimalistas e removendo dependências desnecessárias para o runtime, diminui proporcionalmente a superfície exposta durante o gap. Menos componentes significa menos vetores potencialmente afetados por vulnerabilidades ainda fora do registro público.

Incorporar o processo de disclosure ao modelo de risco:

O tempo de resposta dos vendors ao processo de disclosure afeta diretamente o tamanho do gap. Um vendor que demora semanas para confirmar um report está estendendo o período de exposição não monitorada. Um projeto que recebe o report de uma vulnerabilidade crítica e responde sem data de correção está, na prática, deixando o intervalo aberto indefinidamente. Para componentes de alta criticidade no ambiente, a maturidade do processo de disclosure do vendor responsável é um critério relevante de avaliação, da mesma forma que frequência de atualizações e histórico de resposta a incidentes.

Ajustar como exposição é medida internamente:

o dado relevante para entender a exposição real é quando a vulnerabilidade foi reportada ao vendor, não quando a CVE apareceu no NVD. Esse número raramente aparece em dashboards de security posture porque raramente é coletado. Para organizações que utilizam métricas de segurança para decisões estratégicas, incorporar o intervalo de disclosure como variável explícita no modelo de risco produz uma visão mais precisa da exposição acumulada do que o MTTR calculado a partir da publicação.

Opinião do Especialista

Um aspecto complementar ao disclosure gap é o tempo necessário para que uma vulnerabilidade já divulgada passe a ser efetivamente detectada pelos scanners utilizados pelas organizações. Ferramentas como Grype e Trivy mantêm bancos de dados próprios de vulnerabilidades, construídos a partir de diversas fontes, como NVD, GitHub Security Advisories (GHSA) e advisories de distribuições Linux, e atualizados periodicamente. Assim, mesmo após a publicação de uma CVE, ainda pode haver um intervalo até que ela seja incorporada ao banco de dados do scanner e, posteriormente, até que esse banco seja atualizado no ambiente do usuário. Na prática, isso adiciona uma nova camada de latência entre a divulgação pública da vulnerabilidade e sua detecção efetiva nos processos de varredura. Embora esse comportamento seja o padrão para a maioria dos usuários, organizações com maior maturidade podem reduzir esse intervalo adotando estratégias como a geração e distribuição de bancos de vulnerabilidades próprios ou políticas de atualização mais frequentes.

Matheus Farias

Tech Lead na Getup

Conclusão

O disclosure gap é um fenômeno mensurável: os dados de 133.716 CVEs mostram um ecossistema que melhorou, com a mediana do intervalo caindo 71% entre 2022 e 2026, mas que ainda opera com uma janela estrutural de exposição não monitorada.

Essa janela é maior justamente onde mais importa: nas vulnerabilidades de corrupção de memória, nas CVEs exploradas ativamente e nos componentes de infraestrutura que sustentam a maior parte dos ambientes de produção.

O ponto central dessa discussão é a referência a partir da qual o risco é medido: tratar a data de publicação da CVE como o início da exposição afasta as métricas de segurança da realidade, porque a exposição começa antes e não aparece em nenhum scanner ou SLA enquanto o intervalo está aberto.

Isso não exige reescrever o modelo de disclosure, apenas operar com consciência de que ele existe: reduzir a superfície de ataque, escolher componentes com critério e medir exposição a partir do report, não da publicação.

Heitor Gouvêa
Security Researcher

Sobre esta pesquisa

Esta pesquisa foi conduzida por Heitor Gouvêa. O trabalho teve origem em um conjunto de vulnerabilidades descobertas e reportadas em fevereiro de 2026 em ferramentas amplamente utilizadas no ecossistema de segurança e infraestrutura.

O processo de disclosure desses casos tornou visível, de forma concreta, o intervalo entre a existência de uma vulnerabilidade e sua visibilidade pública, e motivou a análise empírica documentada neste report. Este report é uma síntese executiva dos achados principais, produzida com o objetivo de traduzir os dados em implicações práticas para programas de segurança.

Revisão

Camila Bedretchuk
Head de Produto

Revisão

Marina Mazzuco
Growth Marketing Specialist

Design editorial

Arley Gomes
Product & Web Designer

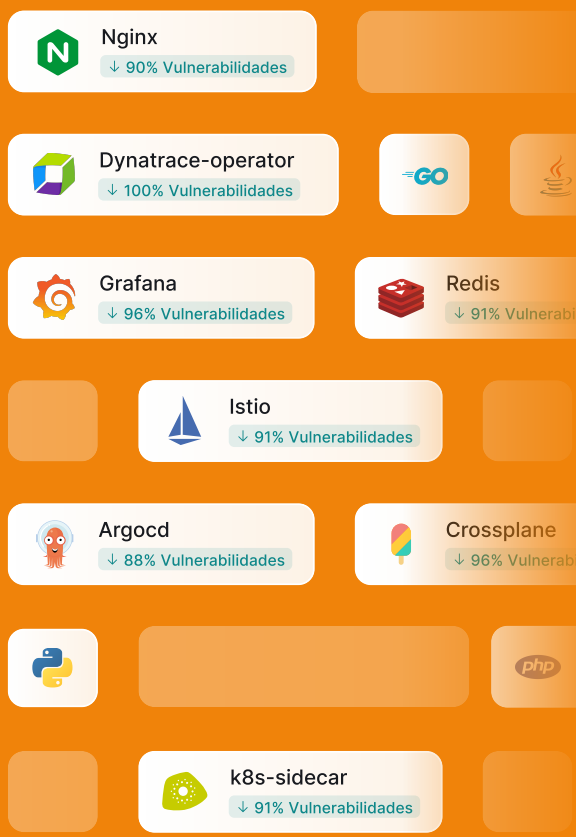
Sobre o Quor

A Getup é uma empresa brasileira especializada em suporte a ambientes Kubernetes e infraestrutura cloud-native. Foi da experiência acumulada gerenciando ambientes de produção para diversas empresas que nasceu o Quor.

O Quor é um catálogo privado de imagens de container construídas com segurança como primeiro princípio. As imagens são compiladas diretamente do código fonte dos projetos upstream, o que permite incorporar correções de segurança antes que as distribuições as empacotem e publiquem. Cada imagem é distribuída com SBOM vinculado ao digest, documentos VEX que distinguem vulnerabilidades exploráveis de ruído de scanner, e atestados de proveniência verificáveis

O catálogo está disponível em: getup.io/quor.

Para organizações que buscam reduzir a superfície de ataque exposta durante o disclosure gap, a escolha dos componentes presentes no ambiente é o ponto de controle mais direto disponível. O Quor foi construído para operar exatamente nessa camada.



Notas & Referências

Notas

1. As tabelas anuais e trimestrais agrupam cada CVE pelo ano de publicação (datePublished), não pelo de reserva. Como todas as CVEs de cada ano já foram publicadas, o intervalo é integralmente observado.

2. Os dados de 2026 vão até 15 de abril e cobrem apenas parte do ano, portanto os números desse ano são preliminares. A mediana tende a ser mais estável; a média e as proporções podem variar conforme o restante do ano for publicado.

Referências

[1] https://github.com/CVEProject/cvelistV5

[2] https://www.wiz.io/blog/ingress-nginx-kubernetes-vulnerabilities

[3] https://www.sonatype.com/state-of-the-software-supply-chain/introduction

[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Glossário

CVSS (Common Vulnerability Scoring System)

Sistema de pontuação padronizado para classificar a severidade de vulnerabilidades de 0 a 10. A pontuação é calculada com base em atributos como vetor de ataque, complexidade de exploração e impacto potencial em confidencialidade, integridade e disponibilidade. É a referência principal usada por scanners e programas de vulnerability management para priorizar remediações

SBOM (Software Bill of Materials)

Inventário estruturado de todos os componentes de software, como bibliotecas, frameworks, pacotes, versões e licenças, usados para construir uma aplicação ou imagem. Permite identificar rapidamente se um componente vulnerável está presente, avaliar o impacto de novas CVEs, atender requisitos regulatórios e de auditoria e gerenciar riscos da cadeia de dependências.

VEX (Vulnerability Exploitability eXchange)

É um formato padronizado de notificação de segurança que permite aos fornecedores de software informar se um componente ou produto específico é realmente vulnerável a uma falha conhecida. Ele funciona como um complemento dinâmico para ao SBOM.

CNA (CVE Numbering Authority)

Organização autorizada pelo programa CVE/MITRE a reservar e publicar identificadores CVE. Pode ser um fabricante, uma empresa de segurança, um projeto open source ou uma entidade governamental.

KEV (Known Exploited Vulnerabilities)

Catálogo mantido pela CISA (agência de segurança cibernética do governo americano) com vulnerabilidades que têm exploração confirmada em ambientes reais. É considerado uma referência prioritária para programas de remediação porque concentra falhas com risco comprovado, não apenas teórico.

MTTR (Mean Time To Repair)

Tempo médio entre a identificação de uma vulnerabilidade e a eliminação do risco em produção (correção aplicada e versão corrigida implantada). No contexto de cadeia de software, abrange as etapas de detecção, análise, priorização, implementação da correção e reimplantação.